Integration Router
with
EasyRouter™ Technology

User's Manual

Part Number 800-1768-60, Rev. A

June 1995

Safety Warning

Access to the interior of the unit for such purposes as fuse replacement, or any other maintenance type of procedure, must only be performed by a qualified technician. Before any such work may be performed, and to avoid any possibility of electrical shock, the power supply cord must be disconnected from the power source.

Notification of FCC Requirements

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Changes or modifications to this product, that could increase the amount of Radio Frequency Emissions from this product, without the expressed written approval of MICOM Communications Corp., could cause the product and the user to violate the FCC's Rules and Regulations, thus requiring the product to be turned off or disconnected.

If this unit is used on a DTE which requires use of shielded cables for compliance with FCC Part 15, then use of a filtered pin connector may be required to maintain FCC compliance. See the Installation section for specific applications.

Notification of Canadian Requirements

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de classe A prescrites dans le règlement sur le brouillage radioélectrique édicté par le Ministère des Communications du Canada.

United Kingdom Requirement: Interconnection of Ports Warning

Interconnection directly, or by way of other apparatus, of ports marked "SAFETY WARNING. See instructions for use", with ports marked or not so marked may produce hazardous conditions on the network. The advice of a competent engineer must be obtained before such a connection is made. None of the ports provide isolation sufficient to satisfy the relevant parts of BS 6301. Apparatus connected to the ports, must either have been approved to the relevant parts of BS 6301 or to have been previously evaluated against BS 6301 British Telecom Technical Guides 2 or 26, and given permission to attach. Other usage will invalidate any approval given to this apparatus.

Any or all of the ports on the following modules may be configured as non-network ports:

- Communications Control Modules (CCM): 6 D-type ports
- Up to 4 Channel Expansion Modules (CEM): up to 6 D-type or 12 RJ45 ports
- LAN modules (including RTS or RLB): AUI, BNC, and 8-pin modular jack ports
- NMS module: 1 log port, 1 command port
- Up to 4 2-port voice cards
- Alarm port

Notice

Specifications, tolerances, and design characteristics described in this manual are subject to change without notice.

© 1995 MICOM Communications Corp.
All rights reserved

Unpublished — rights reserved under the copyright laws of the United States

RESTRICTED RIGHTS LEGEND

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at 252.227-7013.

Safety Warnings and Cautions

The Underwriters Laboratories, Inc. (UL), Canadian Standards Association (CSA), Technische Überwachungsverein (TÜV) of Germany, and British Approval Board for Telecommunication (BABT) request the following statements of warning or caution be made in English, German, and French to help you in the safe operation of the Marathon or NetRunner unit. These statements also apply to any and all modules installed within the Marathon or NetRunner unit.

To ensure adequate cooling of the equipment a 2.0 inch unobstructed space must be maintained around all sides of the unit.

The ac power socket shall be installed near the equipment and shall be easily accessible.

Access to the interior of this unit shall be made only by a qualified technician.

Connection to the network is to be disconnected before the (mains) plug is removed.

Warning

Remove power plug from the power socket before performing any service work on the unit.

Lithium Battery Caution

Danger of explosion if battery is incorrectly replaced. Replace only with the same type or equivalent battery, as recommended by the manufacturer. Discard used batteries according to manufacturer's instructions.

The power supply is auto-ranging in this model.

The power supply cordset to be supplied in Europe must have 0.75^2mm, 3 conductor "HAR" cord type H05VV-F, terminated in a grounding type Shucko plug on one end and a molded – on IEC 320 connector on the other end.

Technical Data

Input Volts	:	100-240 Vac −5%, +10%
Input Current		
Marathon 5K Turbo/10K/20K NetRunner 500ET, 1000E, 2000E	:	3A-1.5A
Marathon 1K, NetRunner 50E, 75E, 100E	:	2A-1A
Frequency	:	47-63 Hz

Um die Kühlung des Gerätes nicht zu beschränken, ist es notwendig um das Gerät herum an allen Seiten ca 5 cm Raum zu lassen.

Stellen Sie das Gerät in der Nähe einer geerdeten Schutzkontaktsteckdose so auf, dass diese leicht erreichbar und zugänglich ist.

Der Zugang ins Innere des Gerätes ist nur einem qualifizierten Techniker gestattet.

Ehe der Netzstecker aus der Steckdose gezogen wird, müssen sämtliche äusserliche Verbindungen vom Gerät getrennt werden.

Warnung

Vor öffnen des Gerätes, muss der Netzstecker aus der Steckdose gezogen werden.

Lithium Batterie Warnung

Explosionsgefahr besteht wenn die Batterie nicht richtig ersetzt ist. Die Batterie darf nur mit einer gleichen oder gleichwertigen Batterie ersetzt werden.

Netzteil ist mit automatischer Umschaltung entsprechend der Versorgungsspannung versorgt.

Die Netzleitung sollte ein harmonisierter Typ (HAR) sein, mit der Bezeichnung H05VV-F oder H05VVH2-F, 3G 0.75^2mm, mit einem Schutzkontakt – und einem Kaltgerätestecker (IEC 320).

Technische Daten

Nennspannung	:	100-240 V∼ −5%, +10%
Nennstrom		
Marathon 5K Turbo/10K/20K NetRunner 500ET, 1000E, 2000E	:	3A-1.5A
Marathon 1K, NetRunner 50E, 75E, 100E	:	2A-1A
Frequenz	:	47-63 Hz

Pour assurer un refroidissement adéquat, maintenir un espace libre de 5 cm (2 pouces) tout autour de l'appareil.

Installer la prise AC à proximité de l'appareil, dans un rayon d'accès facile.

Ouverture de cet appareil est permise par un technicien autorisé seulement.

Avant de débrancher la prise de courant, assurer que toutes les connexions externes ont été déconnecté de l'appareil.

Avertissement

Débrancher la prise de courant avant d'entreprendre aucun travail de réparation de l'appareil.

Batterie Au Lithium Avertissement

Un danger d'explosion existe si la batterie est remplacée incorrectement. Remplacer avec une batterie identique ou similaire, recommandée par le fabriquant. Disposer des batteries utilisées selon la méthode prescrite par le fabriquant.

Ce modèle s'adapte automatiquement au courant électrique ou voltage de la prise murale.

En Europe, brancher l'appareil à la prise murale au moyen d'un fil "HAR" comprenant 3 cables H05VV-F ou H05VVH2-F de 0.75^2mm chacun, avec à une extremité une prise de terre genre SHUCKO et à l'autre une prise IEC 320.

Donnees Techniques

Voltage d'Accès	:	100-240 V∼ −5%, +10%
Courant d'Accès		
Marathon 5K Turbo/10K/20K NetRunner 500ET, 1000E, 2000E	:	3A-1.5A
Marathon 1K, NetRunner 50E, 75E, 100E	:	2A-1A
Fréquence	:	47-63 Hz

WARRANTY

Please make note of MICOM's Warranty for the Integration Router, which is on the facing page. It also includes information about equipment repair by MICOM Customer Service.

PUBLICATION CHANGE REQUEST

At the end of this manual, there is a postage-paid comment form for you to use to suggest an improvement to, point out an error in, or note something you like about this manual. Please feel free to use it. Your input is valuable to MICOM.

TRADEMARKS

MICOM®, Marathon®, NetRunner®, EasyRouter™, FlashPak™, NETMan™, and ®FEATUREPAK are trademarks or registered trademarks of MICOM Communications Corp.

Apple, AppleTalk, EtherTalk, LocalTalk, and Macintosh are trademarks or registered trademarks of Apple Computer Corp.

DEC, DECnet, LAT, ThinWire, and VT are trademarks or registered trademarks of Digital Equipment Corporation.

Ethernet and XNS are trademarks or registered trademarks of Xerox Corporation.

IBM and Token Ring are trademarks or registered trademarks of International Business Machines Corp.

Novell, NetWare, and Internetwork Packet Exchange (IPX) are trademarks of Novell, Inc.

ProComm and PROCOMM PLUS are registered trademarks of Datastorm Technologies, Inc.

UNIX is a registered trademark of UNIX Systems Laboratories, Inc. in the U.S.A. and other countries.

All other names or titles are trademarks of their respective companies.

WARRANTY

MICOM warrants that to the extent that the equipment delivered is hardware, such equipment shall be free from defective material and workmanship for a period of 3 years from the date of shipment of equipment from MICOM when given normal, proper and intended usage. MICOM further agrees to provide, without cost, emergency replacement equipment, shipped freight prepaid, for a period of ninety (90) days from date of shipment of the equipment and factory repair for the remainder of the warranty period provided that:

(a) MICOM is promptly notified upon discovery that the equipment is defective;

(b) The equipment is returned freight prepaid to MICOM;

(c) MICOM's examination of the equipment shall disclose that any defect was not caused by failure of electrical power or air conditioning, damage from lightning or weather-related causes, accident, misuse, neglect, alteration, improper installation, unauthorized repair or improper testing.

To the extent the equipment is or contains software or firmware (collectively "Software"), MICOM warrants that for a period of one (1) year from the date of shipment, the Software shall be free from defects in material and workmanship under normal use and that the programs will perform according to the specifications contained in MICOM's user manual. MICOM does not warrant that the functions contained in the Software will meet a specific requirement or that the operation will be uninterrupted or error free.

INSTALLING NON MICOM SOFTWARE IN MICOM EQUIPMENT SHALL VOID THIS WARRANTY.

MICOM may, in its sole discretion, except for the first ninety (90) days of warranty, elect to repair or replace the equipment, in which event MICOM shall have a reasonable time to make repairs or to replace the equipment. MICOM will return the equipment freight prepaid.

THE PROVISIONS OF THIS WARRANTY ARE IN LIEU OF ANY OTHER WARRANTY, WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL (INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE), AND MICOM'S LIABILITY ARISING OUT OF THE MANUFACTURE, SALE, OR SUPPLYING OF THE EQUIPMENT OR ITS USE, WHETHER BASED UPON WARRANTY, CONTRACT, NEGLIGENCE, PRODUCTS LIABILITY OR OTHERWISE, SHALL NOT EXCEED THE ORIGINAL AMOUNT PAID BY THE BUYER FOR THE EQUIPMENT. IN NO EVENT SHALL MICOM BE LIABLE TO THE BUYER OR ANY OTHER PERSON OR ENTITY FOR UNINTENDED OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR USE DAMAGES) ARISING OUT OF THE MANUFACTURE, SALE OR SUPPLYING OF THE EQUIPMENT.

SERVICE INFORMATION

If you experience difficulty with this product, contact your MICOM Certified Distributor for prompt assistance.

MICOM offers complete factory repair for both in-warranty and out-of-warranty equipment.

Before returning any equipment, you *must* obtain a Return Authorization number. Contact your distributor for assistance.

MICOM warrants all out-of-warranty repairs or upgrades performed at its factory location or performed by MICOM Customer Service for a period of 90 days after completion.

Shipping charges must be prepaid.

MICOM Communications Corp.
4100 Los Angeles Avenue
Simi Valley, CA 93063-3397
(805) 583-8600

Contents

1 – Introduction

Network Code Download 1-1
EasyRouter Technology 1-3
ARP Spoofing 1-5
SAP/RIP Spoofing 1-7
Compatibility 1-9
WAN Compatibility 1-9
LAN Compatibility 1-9
System Compatibility 1-9
Interoperation With Previous Releases 1-11
Terminology 1-12
Symbols 1-12
Basic Operation 1-13
Software 1-13

2 – Connecting the Unit to the Network

Choosing a Location for the Unit 2-1
LAN Ports 2-1
Additional Preliminary Information 2-2
Forming Clusters 2-3
Verify Jumper Settings 2-4
Connect the Units to the LAN 2-5
Connecting to the 8-Pin Modular Jack 2-6
Connecting to the AUI Port 2-6

3 – Startup

Power Up the Unit 3-1
Boot-up Phase 3-2
Normal Operation 3-3
Setting Up For EasyRouter Mode 3-4

4 – Networking Considerations

Overview 4-1
Operation 4-1
Point-to-Point Operation 4-2
Multi-site Operation 4-3
Clusters 4-3
Assigning Integration Routers to Clusters 4-6
Communicating Between Clusters 4-6

Contents

4 – Networking Considerations (continued)

Filtering (point-to-point and multi-site applications) 4-7
Destination Address Filtering 4-7
Address Tables 4-8
Management Filters 4-9
Static Address Filters 4-9
Protocol Filters 4-10
Pattern Filters 4-10
Exclusively Operating Filters 4-10
RARP Protocol Filtering 4-10
The Spanning Tree 4-10
Organization 4-11
Active or Passive 4-11
Interoperation With Traditional Routers 4-12
Management of the Integration Router 4-13

5 – IP Routing

6 – IPX Routing

7 – Command Reference

Command Syntax 7-1
Command Reference Syntax 7-1
Organization 7-2
Bridge Commands 7-5
Set and Define 7-5
ARPBcast Filtering 7-5
ARPSpoof 7-6
ARPSpoof Blocking Thold 7-6
ARPSpoof Blocking Timer 7-6
ARPSpoof Cache_Timeout 7-7
Broadcast 7-7
Cluster 7-7
Compression 7-8
Multicast 7-8
SAPSpoof 7-9
SAPSpoof Blocking Thold 7-9
SAPSpoof Blocking Timer 7-9
Span 7-10
State 7-10
Weed 7-10
Filtering (using SET/DEFINE) 7-11
Exclusive 7-12
Global 7-13
Specific 7-14

Contents

7 – Command Reference (continued)

Show, Monitor, and List 7-15
Addresses 7-15
ARPBlock 7-15
ARPCache 7-16
Counters 7-16
Nodes 7-18
Status 7-19
Traffic 7-20
IP Routing Commands 7-21
Set and Define 7-21
Exclusive Gateway 7-21
Exclusive Network 7-21
Filtering 7-22
Global Gateway 7-22
RIP 7-23
Routing 7-23
Static 7-24
Static Default 7-24
WAN IPaddress 7-25
WAN Subnet Mask 7-25
Show, Monitor, and List 7-26
ARP 7-26
Counters 7-26
IP 7-27
Routes 7-27
IPX Routing Commands 7-28
Set and Define 7-28
Ethernet Frame_Type 7-28
Ethernet Network Number 7-28
Exclusive Network 7-29
Exclusive SAP_Type 7-29
Filtering 7-29
Global Network 7-30
Routing 7-32
WAN Network Number 7-32
WAN Optimize 7-33
Show, Monitor, and List 7-34
Counters 7-34
IPX 7-35
Routes 7-36
SAPS 7-36

Contents

7 – Command Reference (continued)

Server Commands 7-37
Set and Define 7-37
Announcements 7-37
Bootp 7-37
Circuit Timer 7-37
Domain 7-38
Ethernet 7-38
Identification 7-38
Incoming 7-39
IPaddress 7-39
Loadhost 7-40
Lock 7-40
Login Password 7-40
Maintenance Password 7-40
Multicast Timer 7-41
Name 7-41
Nameserver 7-41
Number 7-41
Password Limit 7-42
Privileged Password 7-42
Prompt 7-42
Retransmit Limit 7-43
Software Path 7-43
Subnet Mask 7-43
Show, Monitor, and List 7-44
Characteristics 7-44
Counters 7-45
Status 7-48
General Commands 7-49
CLS 7-49
Connect WAN 7-49
Finger 7-49
Help 7-49
Initialize Server 7-50
Lo 7-50
Lock 7-50
Logout 7-50
Man 7-50
Ping 7-51
Purge Sysdump 7-51
Save 7-51
Set Ports 7-52
Set Privileged 7-52

Contents

7 – Command Reference (continued)

Show/Monitor/List 7-53
Ports 7-53
Sysdump 7-54
Users 7-54
Su 7-54
Test 7-55
Unlock Port 7-55
WAN 7-55
Who 7-55
Zero Counters 7-55

A – Specifications

B – FlashPak Cartridge Installation and Jumper Selection

Safety Information B-2
Installing the LAN Module B-2
Module Location Switch Settings B-2
Installing the EasyRouter FlashPak Cartridge B-3
Setting the Jumpers B-5

C – SNMP Management Information Base

D – Applications

Using Telnet To Access the Integration Router's Command Line Interface . . D-1
Using Integration Routers in IP Routing Mode with Remote LAN Bridges (RLBs) D-2
Filtering IPX SAP Advertisements D-4
Filtering IPX RIP Advertisements D-6
Filtering IP RIP Broadcasts D-8

E – Network Code Download E

Procedure For Code Download Using A PC E-1
Procedures For Code Download Using Bootp or TFTP E-8
Code Download Using Bootp E-8
Code Download Using TFTP E-13

Glossary

Index

Contents

Figures

ARP Spoofing 1-6
SAP/RIP Spoofing 1-8
FlashPak Cartridge Installation 1-13

Cluster Interconnection 2-3
Jumper Settings 2-4
Units on a LAN 2-5
Connection to Twisted Pair Hub 2-6
Connection Using a ThickNet Tap 2-7
Connection Using a BNC Tap 2-7
Connection to a Fan-Out Transceiver 2-8

Indicators 3-2

Point-to-Point Operation 4-2
Multi-site Operation 4-3
Connecting a New Integration Router to Existing Clusters 4-5
Cluster-to-Cluster Communication 4-6
Four Hosts Connected to the Same LAN Segment 4-7
Divided LAN Segments 4-8
Filter Diagram 4-9

Switch S2 and Module Location Settings B-3
FlashPak Cartridge Installation B-4
Setting Jumpers B-5

Table

Indicator Displays During Normal Operation 3-3

Release Notes

Components Of This Release

The Integration Router consists of the following:

- 5000ELI-2 LAN module. This is the circuit board with Ethernet connectors that installs in an Integration unit. For NetRunner 75E, the components that make up the 5000ELI-2 LAN module are part of the 75E's LAN/WAN module.
- EasyRouter HCF FlashPak cartridge. This cartridge plugs into the 5000ELI-2 LAN module to provide Remote Bridge/Router functionality. This cartridge is used with the NetRunner 75E and many models of Integration units. This cartridge can also be used with the previous model of the LAN module (model 5000ELI).
- EasyRouter HCFT FlashPak cartridge. This cartridge is used only with the 5000ELI-2 LAN module and provides Remote Bridge/Router functionality to certain models of Integration units.

New Features

The following new features are included in this release:

- Network Code Download. The Integration Router's operating software is stored in Flash EPROM. The operating software can be updated by downloading from one of the following:
  - a PC connected directly to a CCM asynchronous channel on an Integration unit. The PC in this case can download to any Integration Router in the WAN.
  - a PC connected to an Integration unit using error-correcting modems.
  - using Bootp and TFTP from a server on the same LAN segment as the Integration Router.
  - using NETMan.

  See page 1-1 and Appendix E for more information about Network Code Download.
- IP RIP broadcast filtering. A new set of commands has been added to allow you to control the routes that the Integration Router will learn in TCP/IP networks. The commands are:

```
DEFINE IP EXCLUSIVE GATEWAY
DEFINE IP EXCLUSIVE NETWORK
DEFINE IP FILTERING
DEFINE IP GLOBAL GATEWAY
DEFINE IP GLOBAL NETWORK
```

  See pages 7-21 to 7-23 and D-8 to D-9 for more information on IP RIP broadcast filtering.

- The SET/DEFINE SERVER GATEWAY command has been deleted. This command served no useful purpose for the Integration Router.
- A new command, SET/DEFINE SERVER DOMAIN, has been added. See page 7–38 for information about this command.

Using EasyRouter HCF FlashPak Cartridge With Model 5000ELI LAN Module

The EasyRouter HCF FlashPak cartridge can be installed in the previous version LAN module (model 5000ELI). The EasyRouter HCF FlashPak cartridge incorporates traditional routing of IP and IPX packets, ARP spoofing, SAP/RIP spoofing, and hardware compression for increased throughput. The FlashPak cartridge also provides Network Code Download. The operation of the EasyRouter HCF FlashPak cartridge with the 5000ELI LAN module will be the same as described in this manual, with the following exceptions:

1. There is no 8-pin modular jack for unshielded twisted pair LANs. The 5000ELI LAN module contains a BNC connector for ThinNet LANs.

2. There is no software active port discovery. The LAN port to be used must be selected by jumper, as described in the User's Manual that originally accompanied the module. Thus, active port discovery function discussed on page 3-1 does not operate. Also, the DEFINE SERVER ETHERNET command (page 7-38) does not function.

3. There is no HC (hardware compression) indicator (described on pages 3-2 through 3-3). The HC indicator is provided only on the model 5000ELI-2 LAN module.

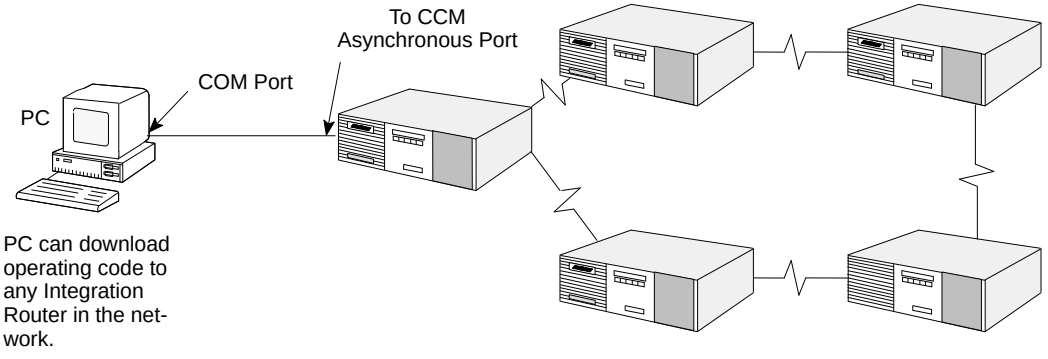
1 Introduction

The Integration Router allows MICOM's Integration products to connect remote LANs over any distance using low-cost leased lines. This permits a device attached to a LAN at one site (say, Los Angeles) to communicate with a device attached to a LAN at another site (New York). The transmission of LAN data for remote sites is in addition to the equipment's integration of data, voice, and fax transmission.

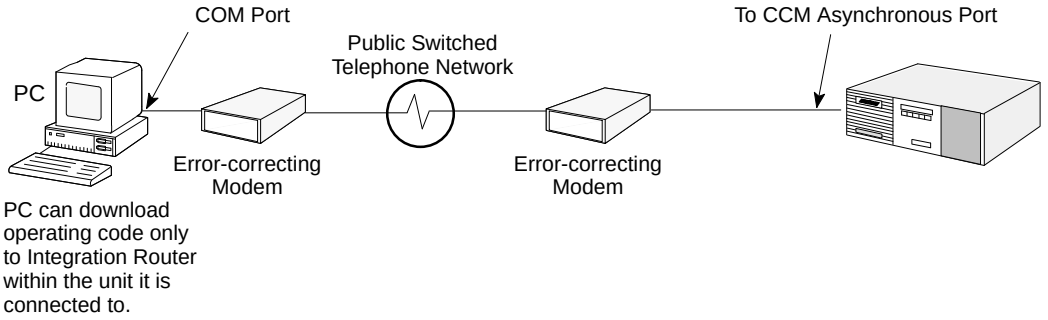
Network Code Download

The Integration Router is equipped with Flash EPROM (FlashPak cartridge). This allows the operating software to be updated without replacing the cartridge. The Integration Router can accept code downloads from:

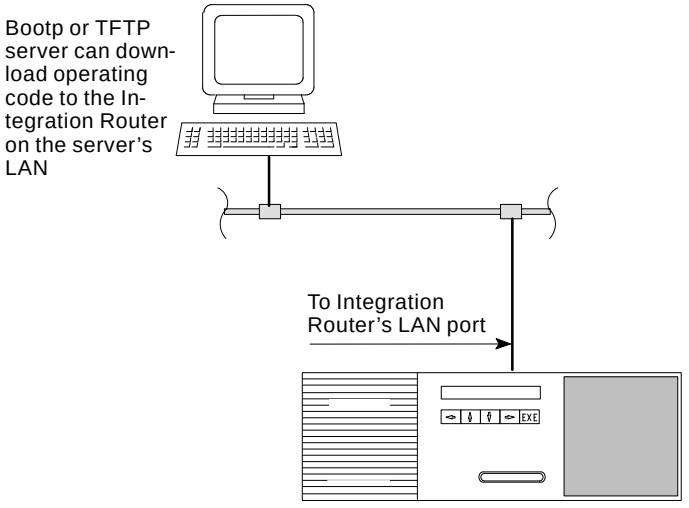
- a PC which is connected directly to a CCM asynchronous channel on an Integration unit. The PC can then download to Integration Routers anywhere on the WAN:



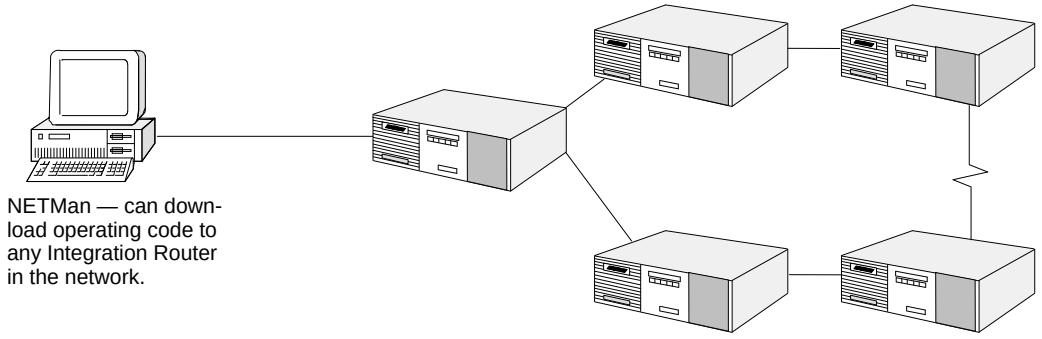
- a PC connected to a remote node using error-correcting modems. In this case, the download is restricted to just the Integration Router in the unit to which the PC is connected:



- using Bootp or TFTP from a server on the same LAN segment as the Integration Router:


Bootp or TFTP server can download operating code to the Integration Router on the server's LAN
To Integration Router's LAN port

- using NETMan release 2.1 or later at a centralized location in the network:



Included with the Integration Router FlashPak cartridge is a 3½″ PC formatted diskette that contains:

1. The Integration Router's operating software.
2. A copy of MICOM's FlashDLD software, DOS version and Microsoft Windows version, that you can use to perform the code download if you do not have a suitable communications program on your PC for performing the code download.

See Appendix E for the network code download procedures.

EasyRouter Technology

The Integration Router includes MICOM's EasyRouter technology. EasyRouter is actually a combination of several technologies that achieve the traffic efficiency and LAN segment isolation of traditional routing, without the effort of network reconfiguration and maintenance. (Traditional routing requires careful network topology consideration and network addressing of all devices. Any changes to the network must be administered to by revising device configurations.)

EasyRouter technology consists of:

- ARP spoofing. For TCP/IP networks, ARP spoofing provides broadcast traffic limiting and storm control. The ARP spoofing agent responds locally to broadcast ARP requests to remote hosts. This traffic is not forwarded across the WAN. ARP spoofing is described in detail on page 1-5.
- SAP/RIP spoofing. For Novell IPX networks, SAP/RIP spoofing provides broadcast traffic limiting and storm control. The SAP/RIP spoofing agent responds locally to SAP/RIP broadcasts. This traffic is not forwarded across the WAN. SAP/RIP spoofing is described in detail on page 1-7.
- WAN optimization. For Novell IPX networks, WAN optimization reduces WAN bandwidth requirements when IPX routing or SAP/RIP spoofing is enabled. When IPX routing, WAN optimization is achieved by sending only RIP table changes between the routers on the WAN – instead of periodically sending the entire RIP table. When SAP spoofing, periodic SAP broadcasts, which are transmitted by all IPX servers, are processed by the Integration Router and only new information is transmitted across the WAN.
- Intelligent multisite bridging. All protocols can be bridged in point-to-point, star, delta, or mesh network topologies. The Integration Router learns which WAN paths lead to specific devices and forwards traffic only across the best paths. The bridge functionality has the following features:
  - Flexible filtering. Packets can be filtered by protocol, source address, or pattern match (see page 4-7 and 7-11 for details about filtering).
  - Self–learning. Automatically learns addresses and locations of network nodes and devices.
  - Spanning Tree. Supports the IEEE Spanning Tree Protocol, to prevent loops in bridged networks.

- Hardware data compression. LAN data is compressed before forwarding across the WAN.
- TCP/IP, LAT, and IPX header compression (in software compression mode only).
- Management. The Integration Router can be managed from:
  - any workstation or terminal attached to an Integral unit
  - a workstation on the LAN using telnet or LAT
  - NETMan
  - SNMP–based network management systems. The Integration Router SNMP Network Management Agent supports monitoring queries (GETs) for most MIB II objects.

The Integration Router also provides:

- TCP/IP multisite routing per RFC 1009.
- IPX multisite routing per *IPX Router Specification*, version 1.10, Novell part number 107–000029–001.

This traditional routing capability is interoperable with other routers, such as Cisco, 3Com, Bay Networks, etc. Interoperability is accomplished by the RIP protocol. See page 4-12 for details about interoperation.

ARP Spoofing

This is a MICOM-developed software algorithm that reduces the amount of broadcast traffic forwarded onto the WAN and prevents ARP broadcast storms in applications where TCP/IP packets are bridged. The default is ARP spoofing is enabled.

Note: The setting of ARP spoofing is ignored when traditional IP routing is turned on. ARP spoofing is active only when the Integration Router is bridging IP packets.

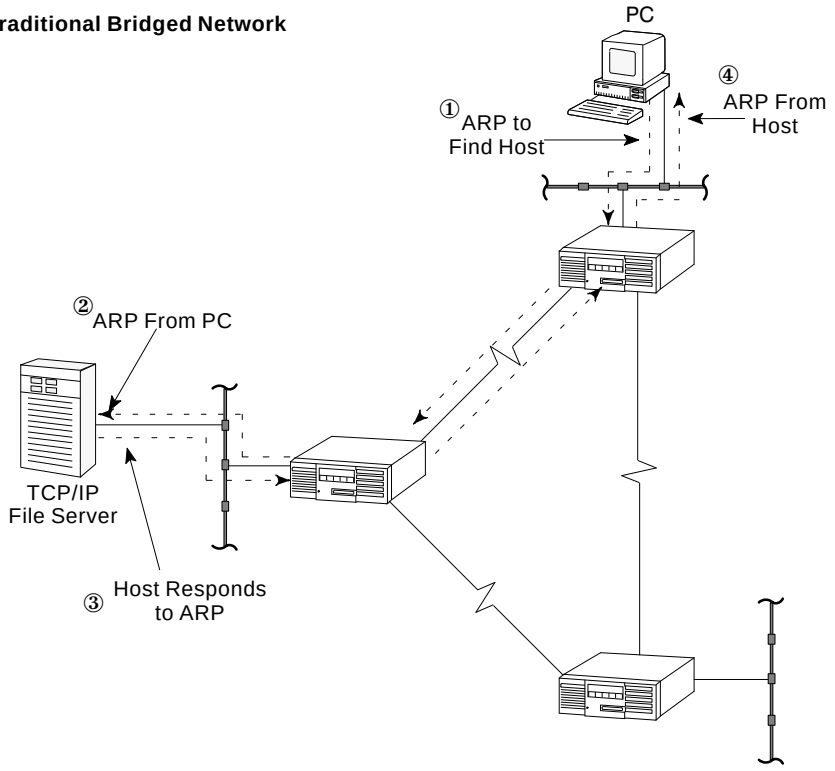
ARP spoofing operates as follows:

- The ARP spoofing agent in the Integration Router learns the IP hosts on the local LAN so it can filter local ARP requests from being forwarded onto the WAN. These ARP requests can be resolved by one of the local hosts. The ARP spoofing agent learns the local hosts by observing only ARP traffic. This is done to prevent degrading the bridge performance of the Integration Router.
- The ARP spoofing agent learns the ARP bindings to remote hosts once a local host establishes a binding with a remote host. After that, requests from other local hosts to that same remote host will be resolved by the ARP spoofing agent. The ARP requests will not be forwarded across the WAN.
- The ARP spoofing agent keeps track of the ARP requests to the remote hosts (across the WAN) and limits the number of outstanding requests to a host per time period. The ARP spoofing agent will allow a certain number of requests to go across the WAN before blocking additional requests to that host until either of the following two events occur:
  - An ARP frame is seen from the remote host.
  - The expiration of a time period.

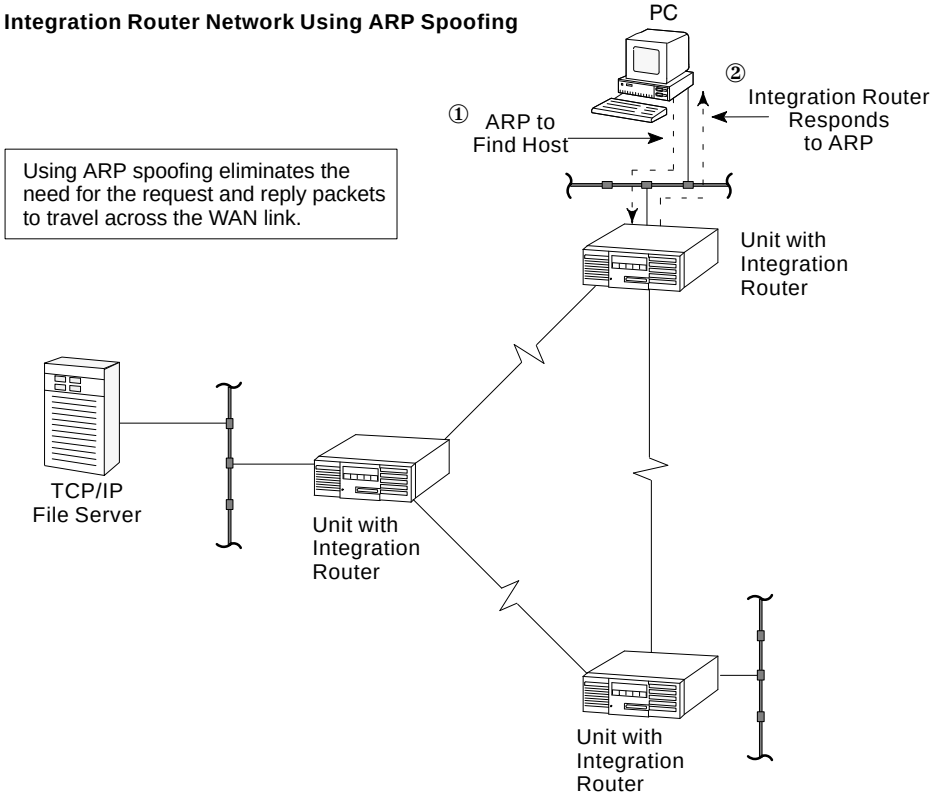
  The number of outstanding requests and the time period are configurable.
- The ARP spoofing agent can optionally filter unsolicited ARP response frames (i.e., ARP response frames with broadcast destination MAC addresses) from being forwarded onto the WAN.

The result of ARP spoofing can be seen in the following illustration:

Traditional Bridged Network



Integration Router Network Using ARP Spoofing


PC
② Integration Router Responds to ARP
① ARP to Find Host
Using ARP spoofing eliminates the need for the request and reply packets to travel across the WAN link.
Unit with Integration Router
TCP/IP File Server
Unit with Integration Router
Unit with Integration Router

ARP Spoofing

SAP/RIP Spoofing

This is a MICOM-developed software algorithm that reduces the amount of broadcast traffic forwarded onto the WAN and prevents broadcast storms in applications where IPX packets are bridged. The default is SAP/RIP spoofing is enabled.

Note: The setting of SAP/RIP spoofing is ignored when traditional IPX routing is turned on. SAP/RIP spoofing is active only when the Integration Router is bridging IPX packets.

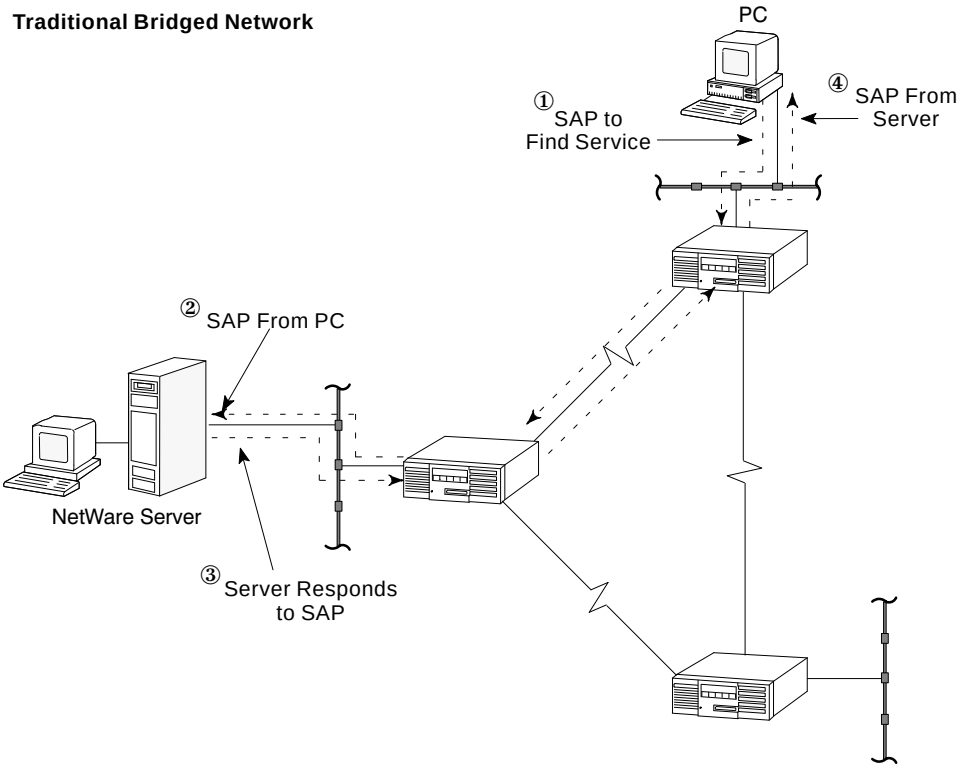
SAP/RIP spoofing operates as follows:

- The SAP/RIP spoofing agent in the Integration Router updates its SAP/RIP tables based on Novell SAP and RIP broadcasts, which are sent out once per minute.
- The SAP/RIP spoofing agent resolves SAP/RIP requests that originate from Novell workstations on the locally attached LAN segment. Any request which can be resolved by the SAP/RIP spoofing agent will not be forwarded onto the WAN.
- The SAP/RIP spoofing agent keeps track of the SAP/RIP requests to the remote hosts (across the WAN) and limits the number of outstanding requests for a particular service type or network per time period. The SAP/RIP spoofing agent will allow a certain number of requests to go across the WAN before blocking additional requests for that service type or network until either of the following two events occur:
  - That service type or network is learned.
  - The expiration of a time period.

The number of outstanding requests and the time period are configurable.

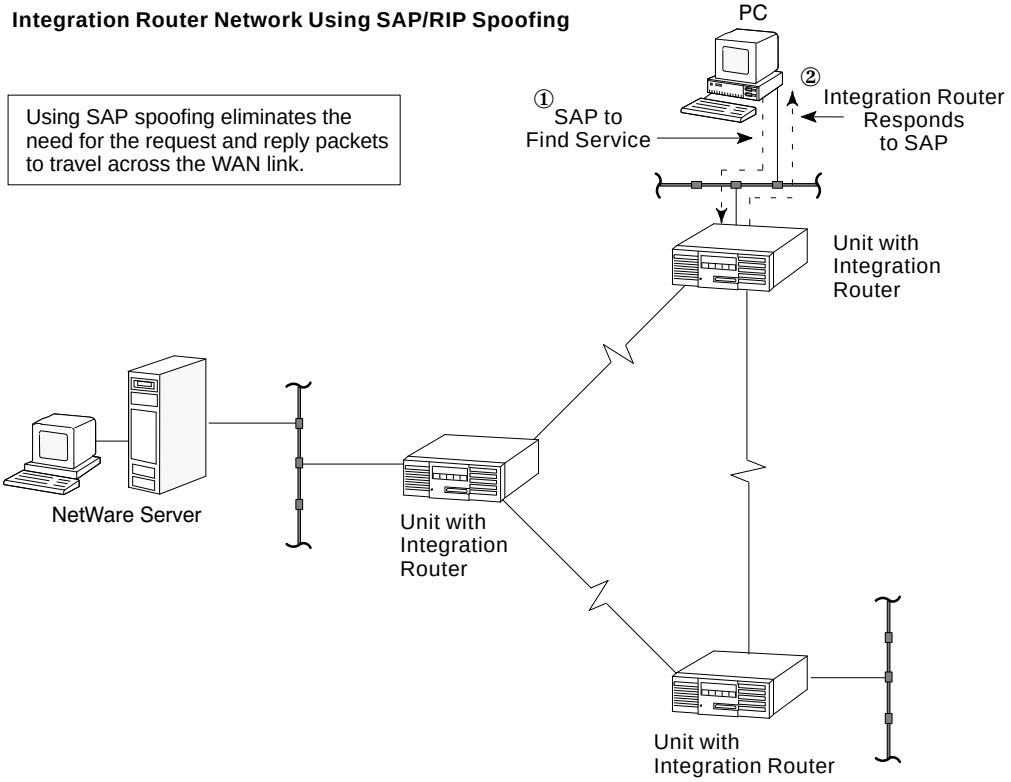
The result of SAP/RIP spoofing can be seen in the following illustration:

Traditional Bridged Network



Integration Router Network Using SAP/RIP Spoofing

Using SAP spoofing eliminates the need for the request and reply packets to travel across the WAN link.



SAP/RIP Spoofing

Compatibility

WAN Compatibility

The Integration Router is WAN compatible with release 3.0 or later of the Marathon Remote LAN Bridge (RLB) and NetRunner products. The LAN modules of all Marathons or NetRunners, which communicate across a single WAN to the Integration Router, must be running software release 3.0 or later. If any of the LAN modules on a single WAN is not running release 3.0 or later software, the network will not operate properly.

The Integration Router ARP, SAP, and RIP spoofing functions are set by default to *enabled*. These settings do not need to be changed, even if some of the other devices on the network do not have this capability. The benefits of ARP, SAP, and RIP spoofing will be limited to those sites that are equipped with the EasyRouter software (Integration Router Releases 5.0 and 6.0).

The Integration Router also has WAN bandwidth optimization set by default to *enabled*. This setting provides the best IPX WAN performance in cases where all devices on a single WAN are running the EasyRouter software. However, you must set WAN bandwidth optimization to *disabled* for all Integration Routers, when a single WAN has devices with earlier LAN module software releases.

LAN Compatibility

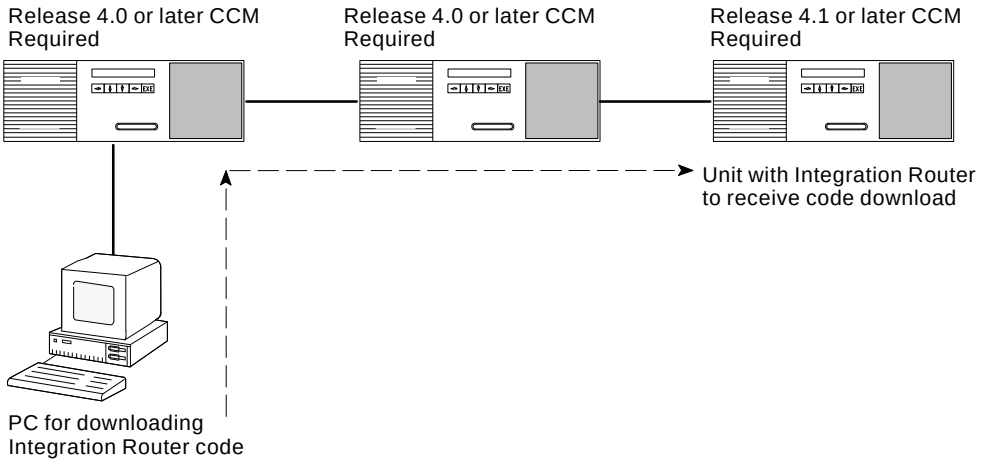
The Integration Router is compatible with all standard bridges, routers, bridge/routers, and other devices that reside on the same Ethernet segment as the Integration Router. The Integration Router is compatible with all previous releases of the RLB and NetRunner across the Ethernet segment, as well.

System Compatibility

For best operation, we recommend that the unit in which the Integration Router is installed be equipped with release 3.2 revision C or later system (Communications Control Module) FEATUREPAK or FlashPak cartridge.

The network code download feature of Integration Router release 6.0 requires that the unit in which the Integration Router is installed be equipped with release 4.1 or later system (Communications Control Module) FEATUREPAK or FlashPak cartridge . If the unit has an earlier release of FEATUREPAK cartridge, the network code download feature will not work. Integration Router release 6.0 in this case will have the same functionality as release 5.0 revision C.

If you intend on downloading the Integration Router code via the WAN, all intermediate nodes must have CCM release 4.0 or later FEATUREPAK/ FlashPak cartridge. If an intermediate node has an earlier release CCM, the code being downloaded will not transit that node properly. The following figure illustrates the CCM release requirements for both intermediate WAN nodes and the ending node containing the Integration Router.


Release 4.0 or later CCM Required
Release 4.0 or later CCM Required
Release 4.1 or later CCM Required
Unit with Integration Router to receive code download
PC for downloading Integration Router code

Interoperation With Previous Releases

RLB/NetRunner Release 3.0 (all revisions)

RLB/NetRunner release 3.0 is equipped with software compression only. It will interoperate across the WAN with all subsequent releases with compression either enabled or disabled. However, when operating over the WAN with RLB/NetRunner release 4.0 or Integration Router release 5.0 revision A, TCP/IP will work properly only if compression is turned off on all devices on the WAN.

RLB/NetRunner Release 4.0 Revision A through Integration Router Release 5.0 Revision A

These releases are equipped with software and hardware compression. They will interoperate across the WAN with all other releases with hardware compression enabled, software compression enabled, or with compression disabled. However, when operating over the WAN with RLB/NetRunner release 3.0, TCP/IP will work properly only if compression is turned off on all devices on the WAN. By default, RLB/NetRunner release 4.0 and Integration Router release 5.0 revision A will run software compression when operating with RLB/NetRunner release 3.0 over the WAN, and hardware compression when operating over the WAN with RLB/NetRunner release 4.0 and all Integration Router releases.

Integration Router Release 5.0 Revision B and C and Release 6.0 (all revisions)

These releases are equipped with software & hardware compression. They will interoperate across the WAN with all releases with no limitations. By default, these releases will run software compression when operating over the WAN with RLB/NetRunner release 3.0, and hardware compression when operating with RLB/NetRunner release 4.0 or greater.

Terminology

- *WAN link* refers to the MICOM WAN network link. In the Command Facility menus, the WAN link is called the interconnect link.
- *WAN port* is any Integration unit port configured as an interconnect link.
- *Integration Router* refers to the combination of a LAN module with an EasyRouter FEATUREPAK or FlashPak cartridge (release 5.0 or later) installed.
- *RLB* refers to the combination of a LAN module plus a Remote LAN Bridge FEATUREPAK cartridge (release 3.0 or 4.0) installed.
- *LAN module* is the circuit board with Ethernet connectors that installs in a unit. It does not have the functionality of an Integration Router or an RLB until the appropriate FEATUREPAK or FlashPak cartridge is installed. Note that for NetRunner 75E, the components that make up the LAN module for other units are part of the 75E's LAN/WAN module.
- *Bridge* refers to two or more RLBs (or Integration Routers in bridge mode) and the WAN link(s) between them.
- A *unit* is any MICOM Integration unit (Marathon, NetRunner, etc.).
- A *cluster* is a group of nodes assigned the same cluster name.
- A *device* is any kind of network equipment (personal computers, servers, printers, etc.).

Symbols

<cr>	Any terminal keyboard key (such as RETURN or Enter) that generates a carriage return.
<break>	Any terminal keyboard key that generates a BREAK signal.
^	Any terminal keyboard key (such as Ctrl) that sets the terminal to shift to the Control character mode.
<esc>	Any terminal keyboard key (such as Esc) that generates an escape character.

Basic Operation

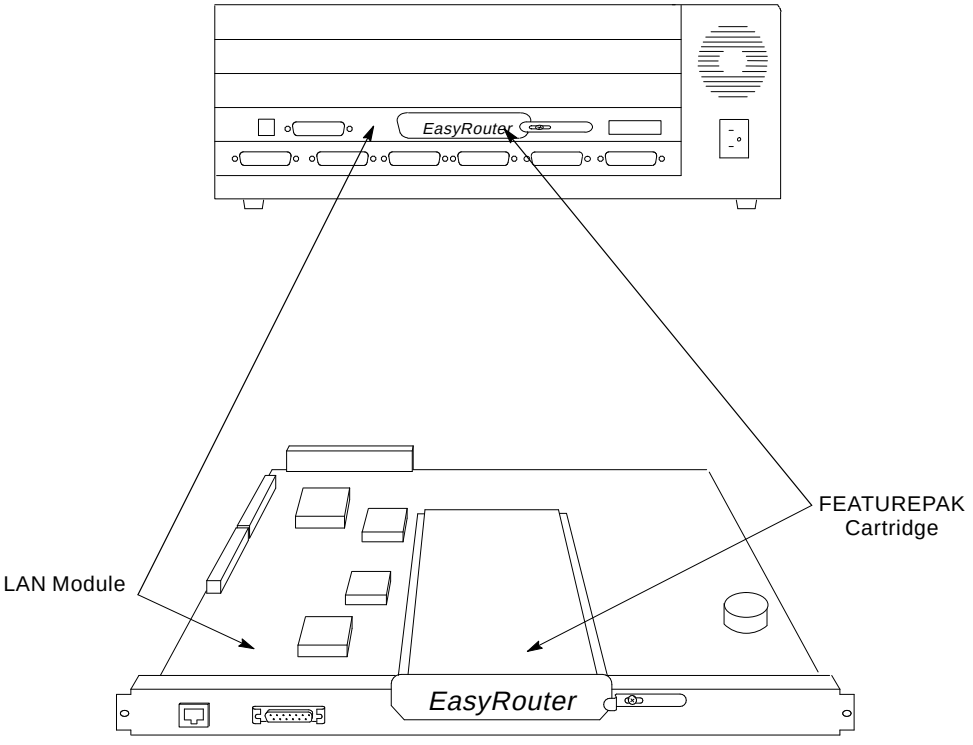
When bridging or in EasyRouter mode, the Integration Router operates at the Data Link layer of the OSI reference model. This means that the Integration Router does not reproduce physical layer network problems like collision or network faults. While bridging, the Integration Router is not protocol sensitive. Data packets travel from the source to the destination node without the Integration Router needing to interpret the data.

When configured for traditional routing, the Integration Router operates at the Network layer of the OSI reference model. The Integration Router can route IP and IPX packets. All other packet types are bridged.

Software

The Integration Router's operation is controlled by the EasyRouter FlashPak cartridge, which is installed directly into the LAN module as shown below.

Note: For NetRunner 75E, please refer to the NetRunner 75E Installation Manual for information on the EasyRouter FlashPak cartridge.



FlashPak Cartridge Installation

Connecting the Unit to the Network 2

If the Integration Router is not already installed in your unit, please refer to Appendix B, *FlashPak Cartridge Installation and Jumper Selection*. Then, return to this section and continue with connecting the Integration Router to the LAN.

Choosing a Location for the Unit

You should consider the following points when choosing a location for a unit that will use the Integration Router:

- Distance between the unit and the LAN cable connection.
- Rear panel accessibility. Removal or replacement of the LAN module's FlashPak cartridge without moving the unit requires at least 12 inches (31 cm) of work space at the back of the unit. For NetRunner 75E, please refer to the NetRunner 75E Installation Manual for the dimensions and locations of the required access areas.

LAN Ports

The required backbone cable, transceivers, transceiver cabling, and connectors should already be in place at the unit location. The LAN module comes equipped with a 15-pin AUI connector and an 8-pin modular jack. All cabling and connectors needed for installation are standard components as specified by IEEE 802.3 and must be supplied by the customer.

Additional Preliminary Information

Prior to connecting the unit to the network, you must gather the following information:

1. How many nodes are interconnected in your WAN? A network of up to 254 nodes can be designed. For networks consisting of more than 12 nodes, you will need to group nodes together in clusters. For networks with 12 or less nodes, clustering is optional. More information on clusters is provided on page 2-3 and in Section 4.

2. Find out your organization's IP or IPX network addressing. If you plan on using the EasyRouter mode or bridging IP packets, you will need an IP address for the Integration Router only if you are going to use SNMP, establish telnet connections to the Integration Router, or perform code download via the LAN. If you plan on traditional routing of either IP or IPX packets, you will need to plan out your network addressing scheme. Network addresses will be required for all devices. Refer to Section 5 for IP routing information and Section 6 for IPX routing information.

3. The LAN module's hardware address is written on a label on its back panel. You should record this number for future reference:

   Ethernet address: `00-40-C5-  -  -`

4. What type of connection will be made to the LAN? For unshielded, twisted pair LANs, you can use the 8-pin modular jack. The LAN module is then connected to a port on a twisted pair hub. For other LANs, you must use the AUI port along with an appropriate transceiver and transceiver cable.

5. What equipment do you need to connect the LAN module to the LAN? The connections are described beginning on page 2-5.

Forming Clusters

A cluster is formed when two or more units are grouped together in the network and given the same cluster name. The default cluster name is <none>. The cluster name is user-configured.

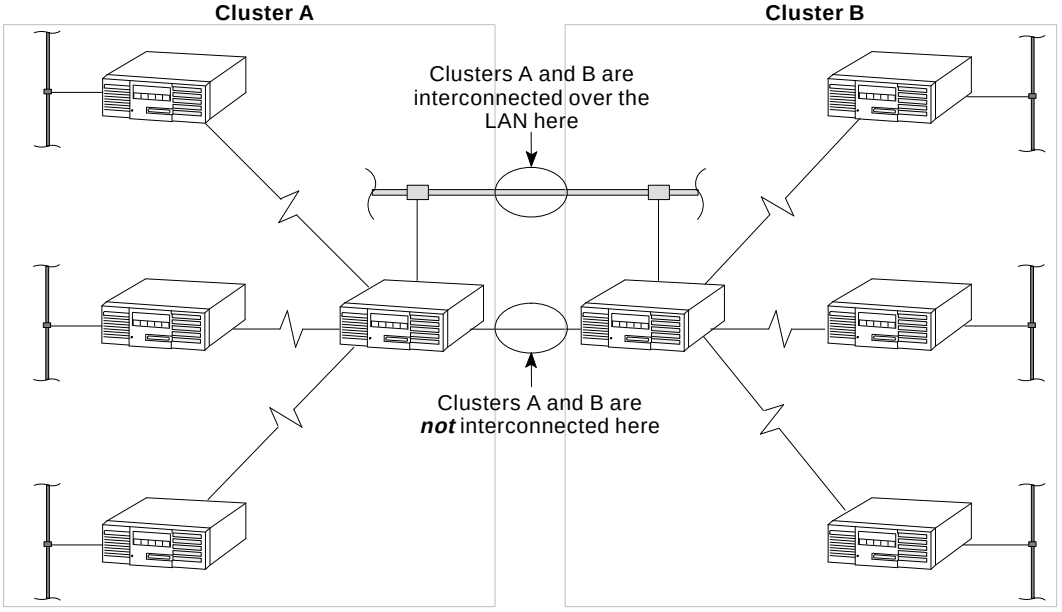
Each LAN module may belong to only one cluster. If a unit contains more than one LAN module, then each LAN module installed in that unit must be assigned to a different cluster.

A single cluster can contain no more than 12 units. If a 13th unit is added to a cluster, it will not be able to communicate. Larger networks (those containing more than 12 units) can be designed by interconnecting clusters.

A cluster segments the network to improve performance and maximize bandwidth for LAN traffic. This is especially true for networks consisting of more than 12 units. It also secures portions of a network by allowing communication only between units with the same cluster name.

Cluster names can be from 1 to 15 alphanumeric characters long. If only one character is desired for a cluster name, it must be an alphabetic character.

Clusters can be interconnected only over the LAN. More information on clusters is provided in Section 3.

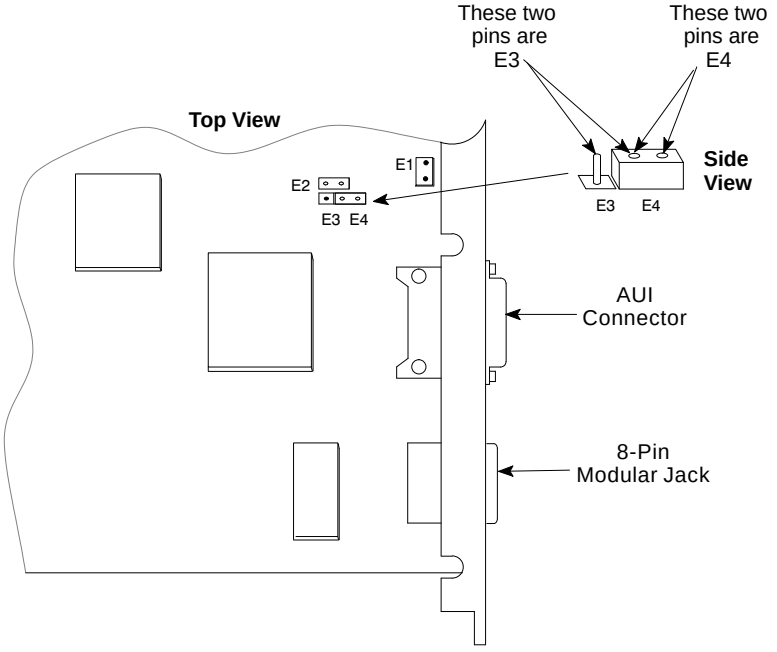


Cluster Interconnection

Verify Jumper Settings

Verify that the jumper configuration is as follows (for NetRunner 75E, please see the NetRunner 75E Installation Manual):

Jumper Locations	Setting
E1	Jumper installed, to enable dc voltages to the AUI connector.
E2	Reserved for future use.
E3/E4	Jumper installed in E4, to enable software active port discovery – requiring no user intervention.

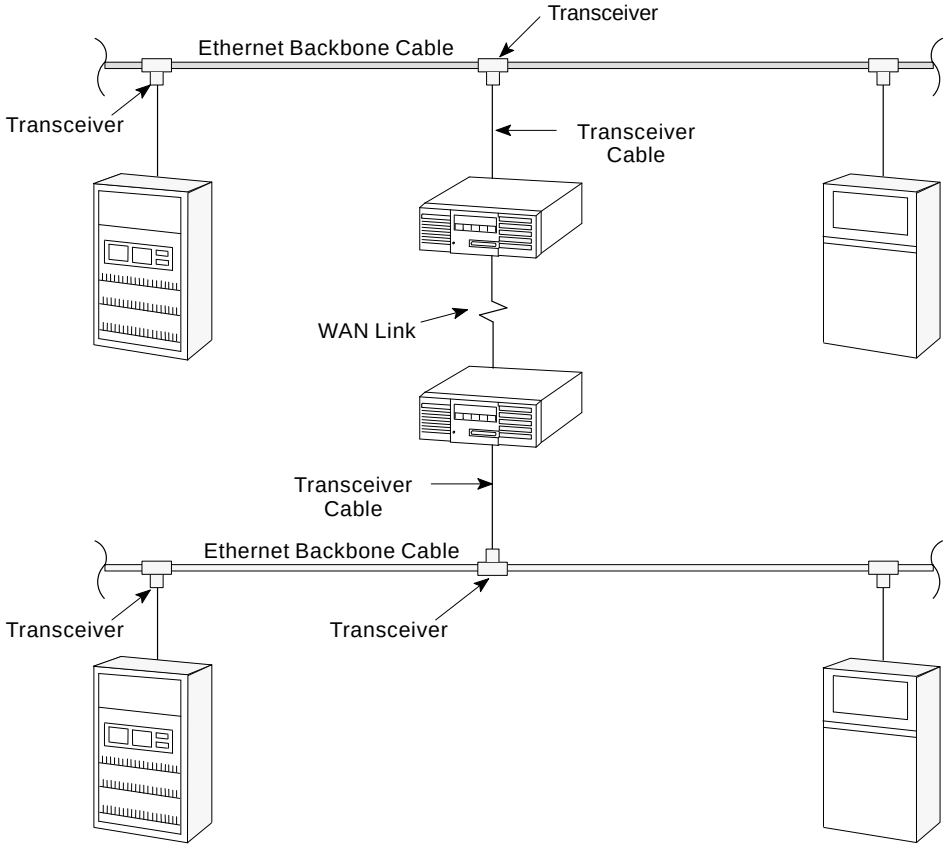


Jumper Settings

To verify the jumper settings, you need to take the cover off the unit and remove as many modules as necessary to view the jumpers. If you need to change the jumper setting, lift off the jumper and move it to the required position.

Connect the Units to the LAN

A unit is connected to the LAN via an IEEE 802.3 standard 10BaseT hub using the 8-pin modular jack, or via a transceiver connected to the AUI port. The figure below shows two LANs connected over the WAN by a pair of units. In the example, the LAN connection is by means of transceiver cables connecting the LAN module's AUI connector to transceivers on the backbone cable.

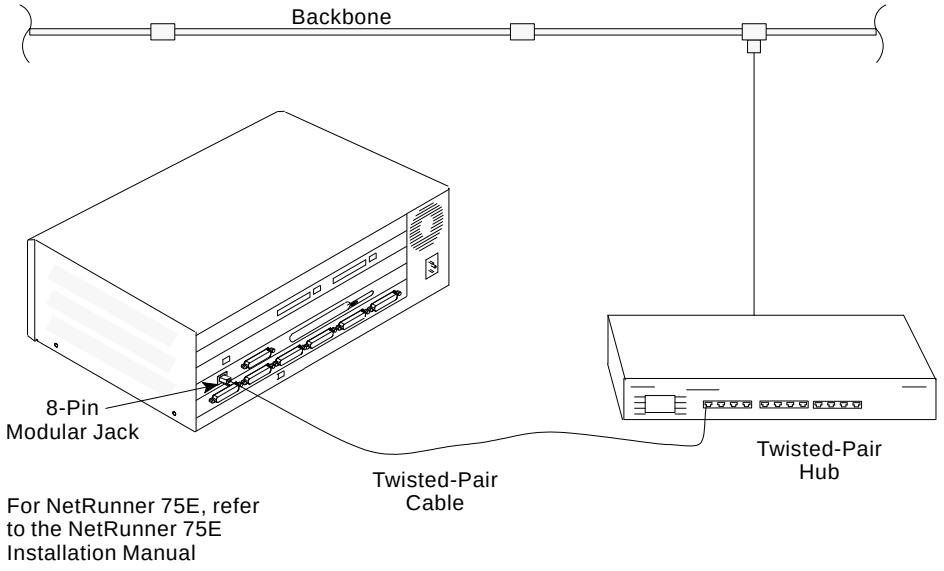


Units on a LAN

The following paragraphs illustrate the various ways of connecting the unit to a LAN.

Connecting to the 8-Pin Modular Jack

Use unshielded twisted pair cable with modular plugs at each end to connect the LAN module's jack to a hub. The hub, in turn, is connected to the backbone.



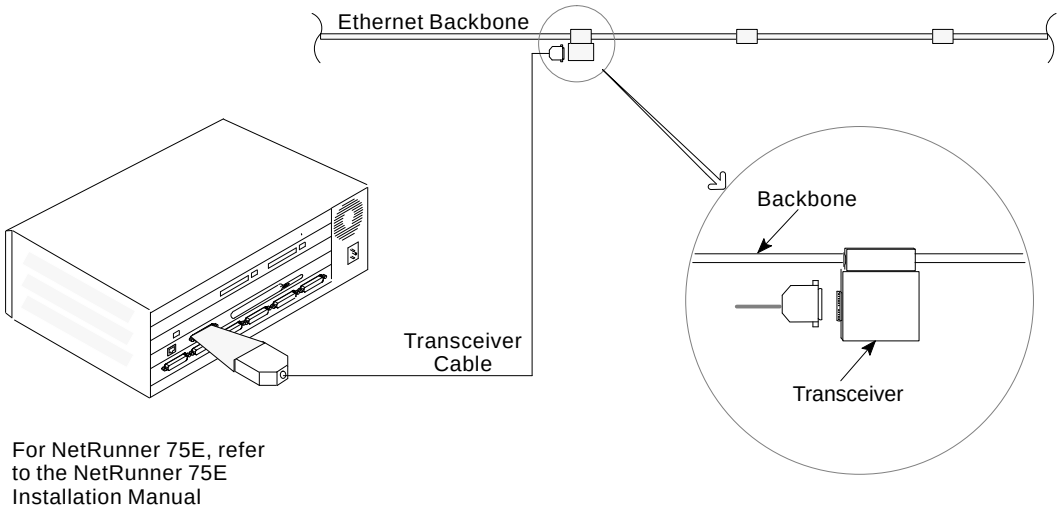
Connection to Twisted Pair Hub

Connecting to the AUI Port

There are several methods for connecting the unit to the LAN using the AUI port:

- Using a shielded cable, connect the unit to the backbone via a transceiver and ThickNet tap as shown in the next figure.

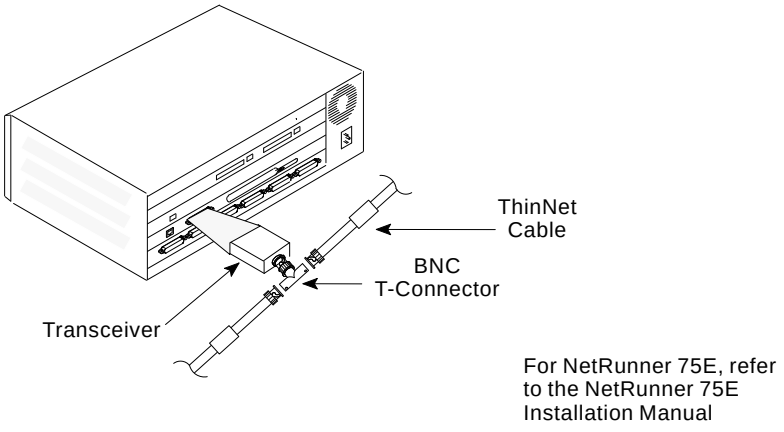
> ⚠ ***CAUTION***
>
> Prolonged breaks in LAN communication can cause network failures. The ThickNet tap in the backbone cable should be installed prior to connecting the unit. If a tap is already present, connecting the unit should have no effect on the network.



Connection Using a ThickNet Tap

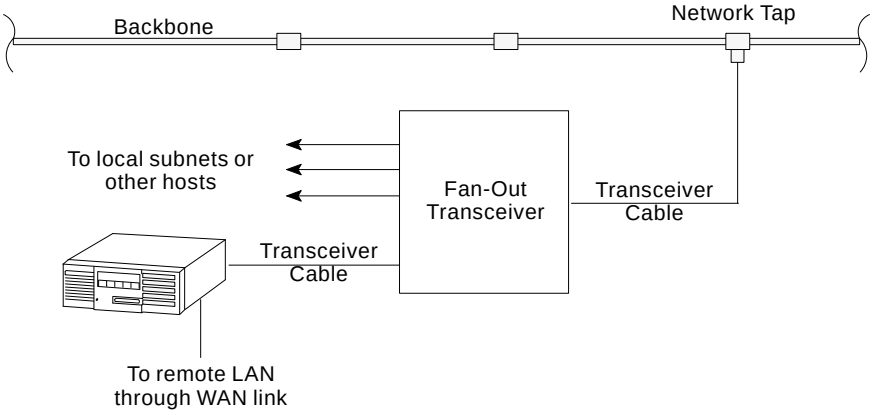
- Connect the unit to a ThinNet LAN using a transceiver with a BNC tap and T-connector as shown in the figure below. If you are attaching the unit at the end of the LAN, you will also need to attach a BNC 50-ohm terminator to the unused side of the T-connector.

Note: Regulatory agencies in some countries may require the installation of a ferrite clamp on the cable within six inches (15 cm) of the transceiver's BNC connector. For a T-type connection, a separate ferrite clamp may be required on each side of the BNC connection. Consult your local regulatory requirements. No clamp-on ferrite is required for installations within the U.S.A.



Connection Using a BNC Tap

- The unit may also be attached to the LAN using interconnect devices such as a hub or fan-out transceiver. The next figure shows the unit connection using transceiver cables and a fan-out transceiver connected to a single backbone tap. **Fan-out transceivers are also known as multiport transceivers.**



Connection to a Fan-Out Transceiver

These are the most common methods for connecting your units to a LAN. In some cases, different connections may be required for special network architectures. The units are compatible with any standard IEEE 802.3 connection. For questions regarding other connection capability, contact your MICOM Certified Distributor.

Startup 3

Power Up the Unit

1. Connect the LAN module to either a 10BaseT hub (using unshielded twisted pair cable) or to a transceiver, as described in Section 2. At this point, the LAN does not have to be operational. The LAN module simply needs to see a device on either the AUI connector or the 8-pin modular jack.

2. Plug the power cord into the back of the unit and into the wall outlet. On power-up, the Integration Router will automatically go into a self-test mode.

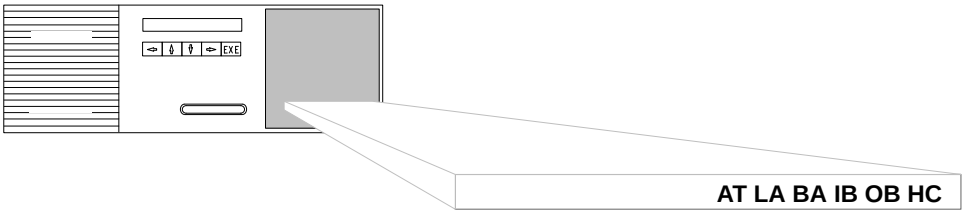
Notes:

a. The Integration Router's self test requires a terminated connection to one of the LAN ports (AUI/10BaseT). This terminated connection is necessary so that the active port discovery function can select the correct port and the self test can successfully complete.

b. If the self test fails to complete, the test will be repeated two more times (for a total of three tries). After three attempts, if the self test still is not successful, further testing will stop and the Integration Router will not operate. In this case, disconnect power from the unit and check the LAN connection. Repeat steps 1 and 2. If the Integration Router still fails to come up, contact your MICOM Certified Distributor for assistance.

Boot-up Phase

The boot-up phase consists of a test sequence and a learning phase. The test sequence is displayed on the indicators on the front panel of the module.



For NetRunner 75E, refer to the NetRunner 75E Installation Manual

Indicators

Upon successful completion of the test sequence, the Integration Router enters a learning phase that lasts approximately 50 seconds. During this time, no packets are passed. Instead, the Integration Router learns the identity of the nodes and devices connected to its LAN and enters this information in an address table (see Section 4, Filters, for details on the address table). In addition, the Integration Router attempts to establish contact with any bridges or routers located within the remote units at the opposite ends of the WAN links.

Normal Operation

Once the learning phase of the power-on sequence is complete, the Integration Router begins normal operation over the network. The following table lists the states of each indicator during normal operation.

Indicator Displays During Normal Operation

Indicator	Function	Description
AT	Power On	Should remain on while the unit is powered on. Blinking indicates an error state.
LA	LAN Activity	Blinks when an Ethernet packet is detected on the WAN or LAN. Also blinks during Bootp, TFTP code downloads.
BA	Bridge/Router Activity	Blinks when the Integration Router communicates with the LAN processor. Also blinks during code download, when a data block is being acknowledged.
IB	Input Buffer	Blinks when the Integration Router receives a packet from the CCM. Also blinks during WAN/CCM code download.
OB	Output Buffer	Blinks when a packet is transmitted from the Integration Router to the CCM.
HC	Hardware Compression	Is turned on when this local LAN module has the EasyRouter FlashPak cartridge installed.

A special state is displayed as follows:

AT = Off
LA = On
BA = On
IB = On
OB = On
HC = Off

This means an incorrect cartridge is installed in the LAN module.

Setting Up For EasyRouter Mode

The Integration Router's parameters default to those settings required for EasyRouter mode. These settings are also suitable for traditional bridging. For initial startup into EasyRouter mode, perform the following at each newly installed Integration Router in the network:

1. Make sure that all units in your network have:
   a. Node numbers assigned to them.
   b. The interconnect links are configured and operational.

   If necessary, refer to the WAN user documentation that accompanied your units for procedures on setting up the above.

2. Select the Integral LAN Local Mode Access option from the unit's Command Facility Main Menu, as follows:

```
COMMAND FACILITY MAIN MENU [node id]

11  INTEGRAL LAN LOCAL MODE ACCESS
```

Enter the letter that corresponds to the location of the Integration Router Module within the unit.

```
ENTER MODULE LOCATION [B–E] (^X TO ABORT):
```

You will receive the Integration Router prompt for command entry. Enter a user name.

```
Username>
```

```
Local>
```

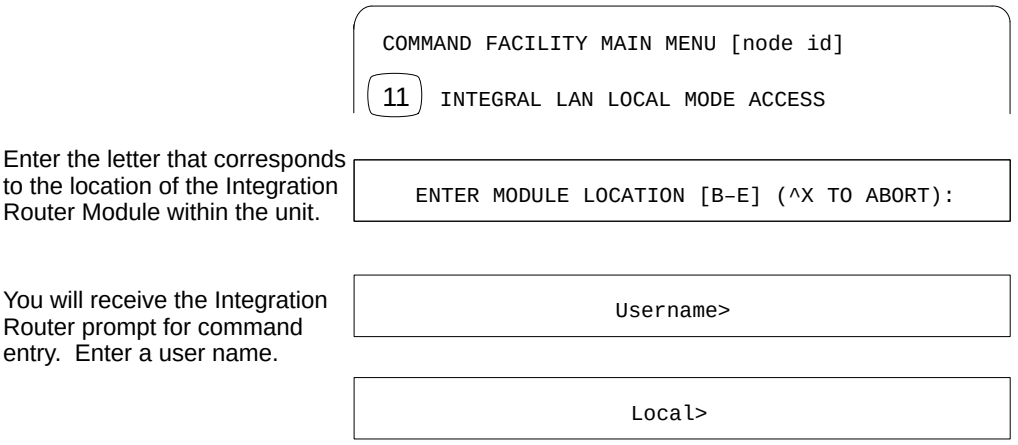
3. This step is optional. If there are more than 12 nodes in the WAN (that is, units with Integration Routers – each Integration Router Module counted as one node), you must group the nodes into clusters of no more than 12 nodes per cluster. If you have less than 12 nodes in the WAN, you can skip this step. (For more information about clusters, see page 4-3.)
   a. Define names for each cluster. The default name is NONE, which you can continue to use. For each node of the other clusters, you must assign it a different cluster name.
   b. Assign the Integration Router to a specific cluster by entering the following command at the Local> prompt:

      ```
      DEFINE BRIDGE CLUSTER clustername
      ```

      (where *clustername* is the name chosen for this node's cluster)
   c. Reset the Integration Router to put the cluster name into effect by entering the following command at the Local> prompt:

      ```
      INITIALIZE SERVER DELAY 0
      ```

The Integration Router will reset and return the display on your terminal to the Command Facility Main Menu. Access the Integration Router command line as follows:


COMMAND FACILITY MAIN MENU [node id]
11 INTEGRAL LAN LOCAL MODE ACCESS
Enter the letter that corresponds to the location of the Integration Router Module within the unit.
ENTER MODULE LOCATION [B–E] (^X TO ABORT):
You will receive the Integration Router prompt for command entry. Enter a user name.
Username>
Local>

4. At the Local> prompt, enter:

   SHOW BRIDGE

   You will see a display similar to the following. The important parameters that you should check are highlighted.

```
Local> show bridge
Current Bridge Configuration                  Cluster/Node           <None>:-3
   Hello Time:       2     Forward Delay Time:   15     Weed Time:        300
   Lan State:  Forward     Maximum Age:          24     Path Cost:          0

Root Bridge: 0x8000, 00-40-c5-00-00-00 ,-1  Spanning tree: Enabled

Global Characteristics: Broadcasts  Multicasts  Compression

Arp Spoofing                                    enabled
Arp cache timeout                               600
ArpSpoof block timeout                          20
ArpSpoof block threshold                        6
Bridging of unsolicated arp responses           enabled

Ipx RIP & SAP Spoofing                          enabled
SapSpoof block timeout                          20
SapSpoof block threshold                        3

Global Address Filters:                         None.
Global Protocol Filters:                        None.
Global Pattern Filters:                         None.
Specific Filters:                               None.

Local> _
```

5. In the Current Bridge Configuration display, verify that the LAN State is FORWARD. (It may take a full minute after reset before the LAN state is set to FORWARD.) If so, the Integration Router is operating properly and forwarding Ethernet packets across the WAN. In that case, you can skip to the next step.

   If the LAN State is DISAB (or, disabled), check the following:

   a. Verify that the jumpers on the LAN module are set correctly (see page 2-4 for information on the LAN module jumpers).

   b. Make certain you have a secure LAN connection to the Integration Router's LAN port.

   c. Make sure that the bridge mode is enabled, by entering the following commands:

      ```
      SET BRIDGE STATE ENABLE
      SAVE BRIDGE
      ```

   d. In the Current Bridge Configuration display, verify that BROADCAST and MULTICAST in the Global Characteristics field are displayed as shown in the example above. If `(NO)` is displayed in front of either BROADCAST or MULTICAST, enter the following command sequence:

      ```
      SET BRIDGE BROADCAST ENABLE
      SET BRIDGE MULTICAST ENABLE
      SAVE BRIDGE
      ```

   e. Manually select the correct Ethernet port by entering either of the following commands:

      ```
      DEFINE SERVER ETHERNET AUI
      ```

      (to enable the AUI port)

      ```
      DEFINE SERVER ETHERNET UTP
      ```

      (to enable the 8-pin modular jack)

   Then, initialize the Integration Router by entering the following command:

   ```
   INITIALIZE SERVER DELAY 0
   ```

   And repeat steps 1 through 4 after the LAN module has finished resetting to verify that the Integration Router is now in a forwarding state. If the Integration Router is still not forwarding, contact your MICOM Certified Distributor for assistance.

6. Verify that the Integration Router is in the EasyRouter mode, as follows:

   EasyRouter Mode:

   Bridge State = enabled
   Broadcast = enabled
   Multicast = enabled
   IP Routing = disabled
   ARP Spoofing = enabled
   IPX Routing = disabled
   SAP/RIP Spoofing = enabled

   a. In the Current Bridge Configuration display (shown on page 3-5), verify that **Arp Spoofing** is **enabled**. If not, enter the following at the Local> prompt:

      ```
      DEFINE BRIDGE ARPSPOOF ENABLED
      ```

   b. In the Current Bridge Configuration display, verify that **Ipx RIP & SAP Spoofing** is **enabled**. If not, enter the following at the Local> prompt:

      ```
      DEFINE BRIDGE SAPSPOOF ENABLED
      ```

   c. Then, reset the Integration Router to enable ARP and SAP/RIP spoofing by entering the following command at the Local> prompt:

      ```
      INITIALIZE SERVER DELAY 0
      ```

   The Integration Router is now in EasyRouter mode. Note that the Integration Router in a traditional bridge state would be represented as follows:

   Traditional Bridge Mode:

   Bridge State = enabled
   Broadcast = enabled
   Multicast = enabled
   IP Routing = disabled
   ARP Spoofing = disabled
   IPX Routing = disabled
   SAP/RIP Spoofing = disabled

The following two parameters are optional, but you may wish to set them at this time.

- If you want to use TCP/IP protocol to access the Integration Router (for example, using telnet or SNMP), you must set the Integration Router's IP address. Enter the following command at the Local> prompt:

  ```
  DEFINE SERVER IPADDRESS ip_address
  ```

  (for example, *define server ipaddress 192.53.139.200*)

  Then, reset the Integration Router to make the new IP address effective by entering the following at the Local> prompt:

  ```
  INITIALIZE SERVER DELAY 0
  ```

- If you want to access the Integration Router using the LAT protocol, you must set a LAT server name for the Integration Router. Enter the following commands at the Local> prompt:

  ```
  SET SERVER NAME name
  SAVE SERVER
  ```

If you wish to set the Integration Router for traditional IP or IPX routing, see Section 5 (IP Routing) or Section 6 (IPX Routing).

Networking Considerations 4

Overview

Bridges and routers operate transparently to LAN users, including the equipment users at either side of the WAN network link. Following power-on and learning phases, data packets pass between LANs in either direction. Normally, the equipment operator may monitor the LAN traffic from time to time by observing the action of the indicator lights described on page 3-3, but will otherwise not need to be involved in the operation.

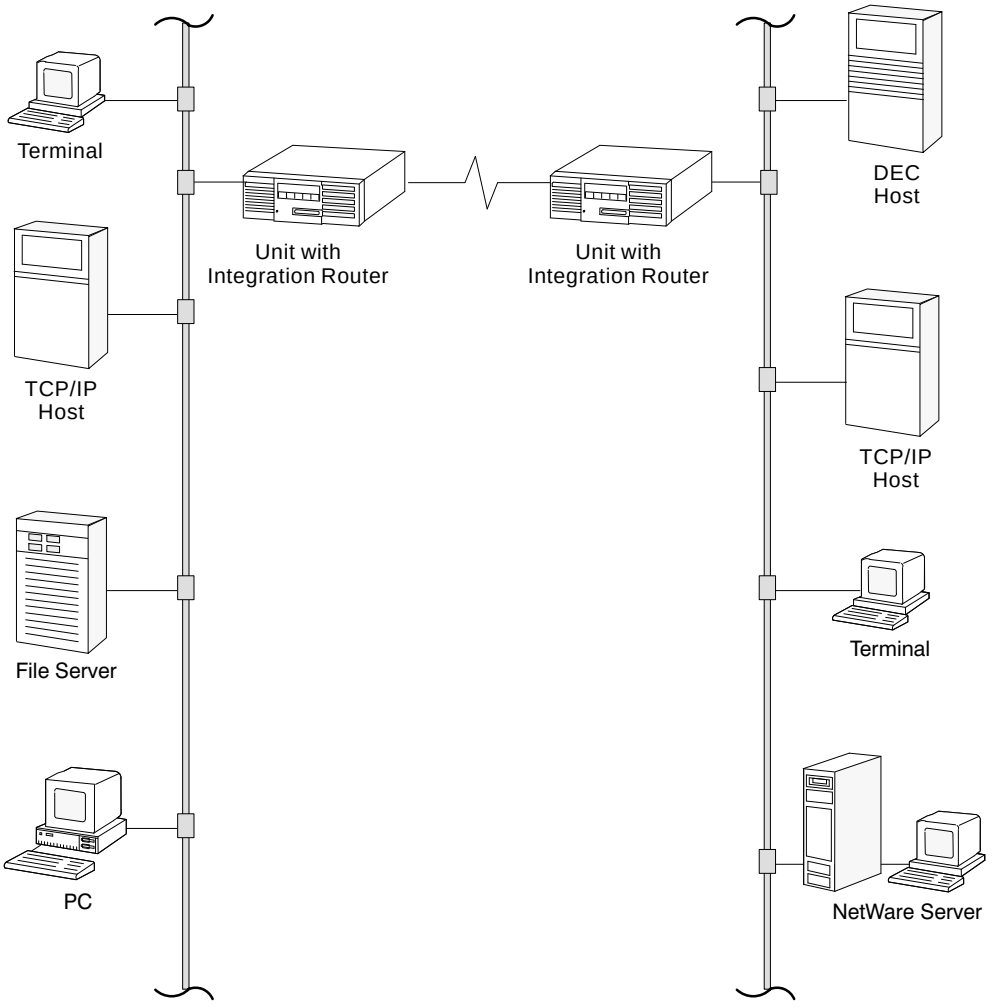
With the exception of a malfunction, operator intervention will be required only to reconfigure the units or to obtain a display of existing parameters. These actions can be performed from a LAN device like a terminal or PC, or from the command console at any unit.

Operation

The units isolate network traffic, effectively controlling (filtering) the amount of traffic traveling between segments (across the WAN network link), which reduces overall network traffic. The Integration Router automatically discovers the other bridges and routers during the learning phase of the unit start-up sequence.

Point-to-Point Operation

In a point-to-point application as shown below, a link is formed between two Integration Routers across a WAN network. Packets are forwarded between the two nodes. Filters may be set for specifying which types of packets each Integration Router accepts or ignores.

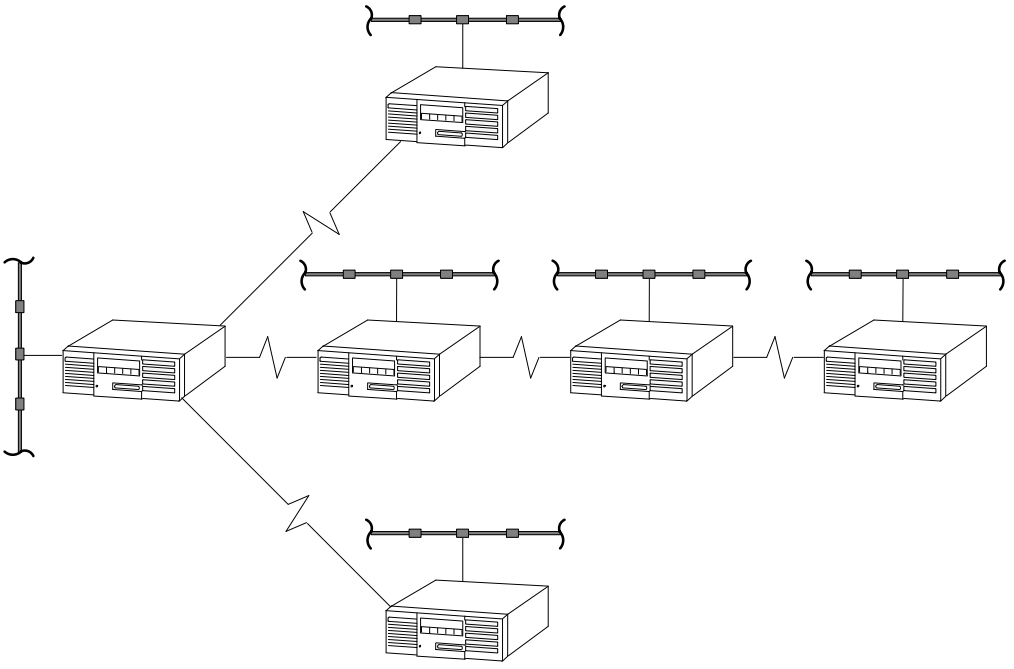


Point-to-Point Operation

Multi-site Operation

The Integration Router and RLB Releases 3.0 and above support multi-site operation. Rather than a simple connection between only two units, and subsequently an interconnection between only two LANs, multi-site operation supports distributed LAN topologies, allowing interconnection between multiple units (see the example shown in the figure below). In addition, Integration Routers and RLBs may be grouped into clusters of up to 12, and clusters connected over a common LAN (refer to *Clusters*, below) so that both small and large wide area networks are supported.

The following subsections: *Clusters, Assigning Nodes to Clusters,* and *Communicating Between Clusters* detail multi-site operation. The sections *Filtering* and *The Spanning Tree* also apply to multi-site applications.



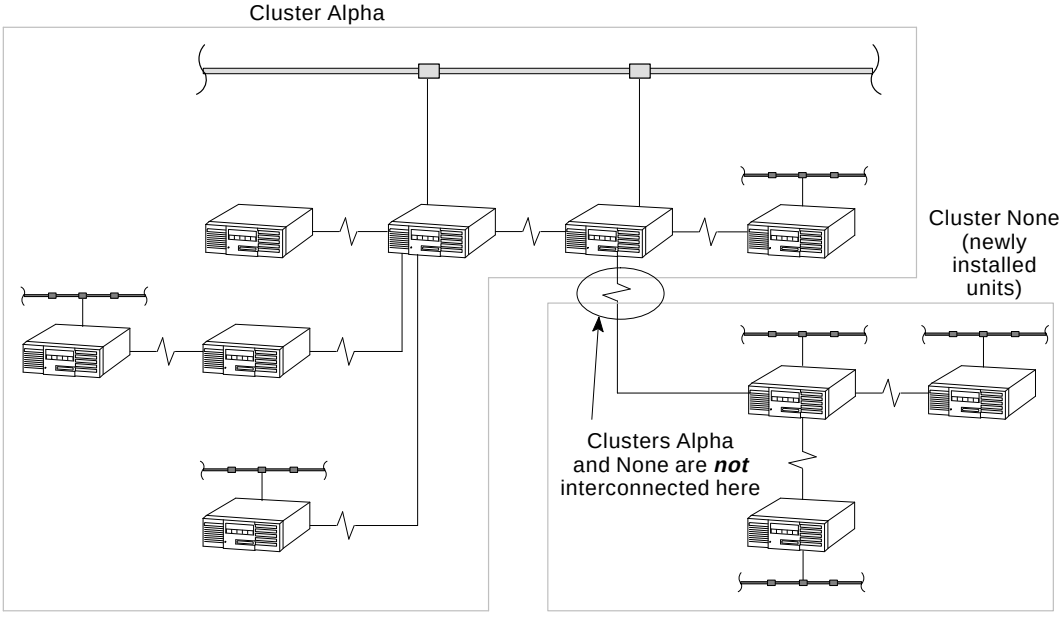
Multi-site Operation

Clusters

The Integration Router allows a network to be partitioned into groups called clusters. A single cluster may contain up to 12 interconnected units on a WAN. Configuring multiple clusters allows you to create a WAN exceeding 12 units, up to a maximum of 254 units per WAN. Clustering, as mentioned here, allows you to efficiently expand your network.

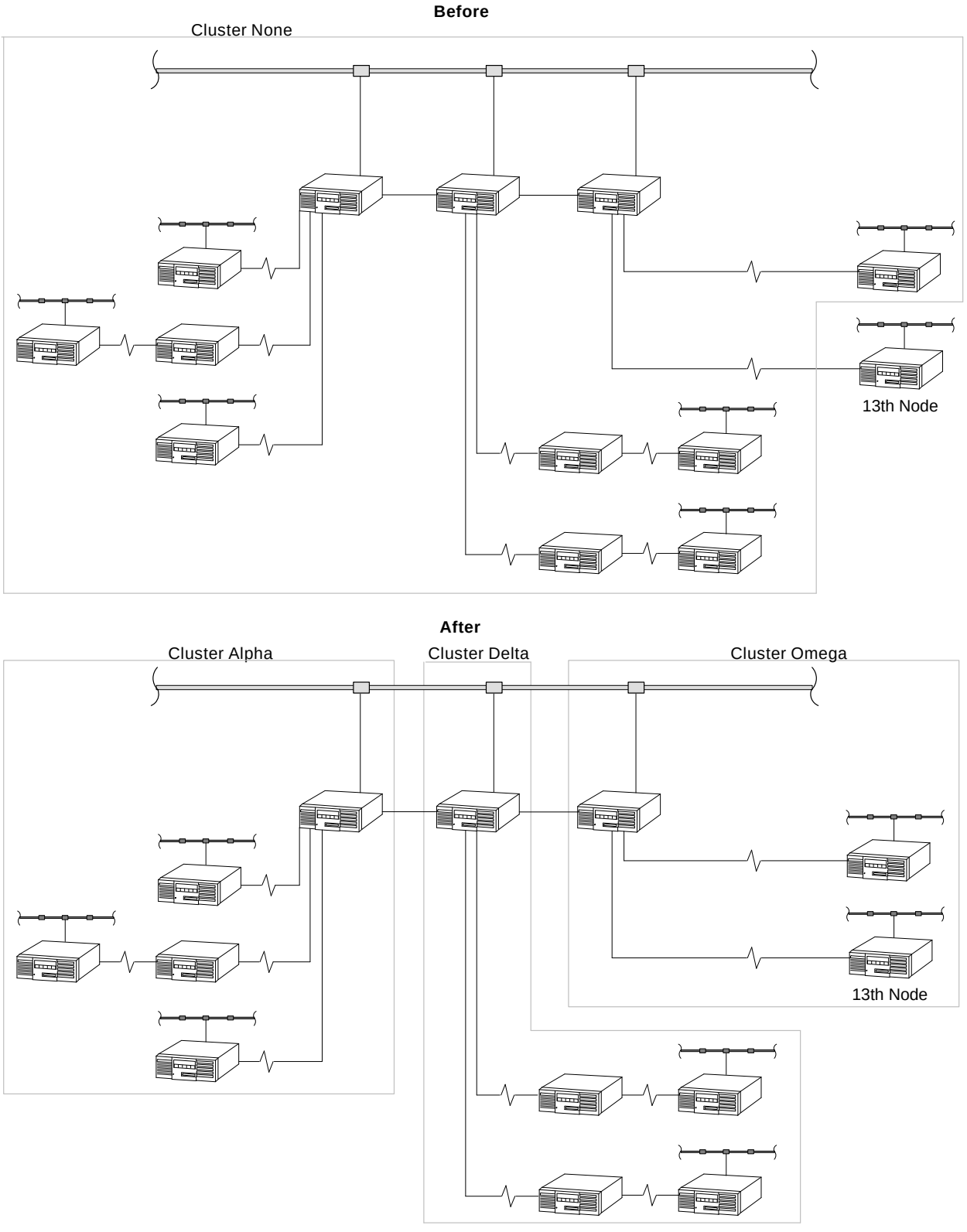
When first powered on, a newly installed Integration Router automatically attempts to establish connection with up to 11 interconnected Integration Routers and RLBs (during the learning phase). The following needs to be taken into consideration when connecting a new Integration Router to a network:

- Each Integration Router and RLB may belong to only one cluster. (Units containing two Integration Router Modules count as two nodes. The two Integration Routers can be assigned to one cluster and count as two nodes in that cluster, or they can each be assigned to different clusters and count as one node in each cluster.)
- A new Integration Router will only attempt connection via the WAN with other Integration Routers and RLBs assigned to the default cluster name of <*none*>. Integration Routers and RLBs assigned to other clusters will be ignored. For example, newly installed Integration Routers, as shown in the figure, will only connect to nodes in cluster None. The remaining nodes have been assigned to a different cluster (Alpha) and are ignored by the new Integration Routers. To connect a new Integration Router to the Alpha cluster, its cluster name needs to be changed, as described in the next subsection.



- Each cluster may consist of up to 12 interconnected Integration Routers and RLBs. For example, if you connect a new Integration Router to a WAN with 12 nodes already in place, a request for connection by the new Integration Router will be ignored, as each node's address table already holds the maximum of 11 other node addresses.

  To add the new node to the network, the original 12 nodes need to be partitioned into smaller clusters and the new Integration Router assigned to one cluster or another. This is illustrated in the following figure.



Connecting a New Integration Router to Existing Clusters

Assigning Integration Routers to Clusters

To assign an Integration Router to a particular cluster, access the Integration Router as described in Section 3. At the Local> prompt, type:

```
DEFINE BRIDGE CLUSTER clustername
```

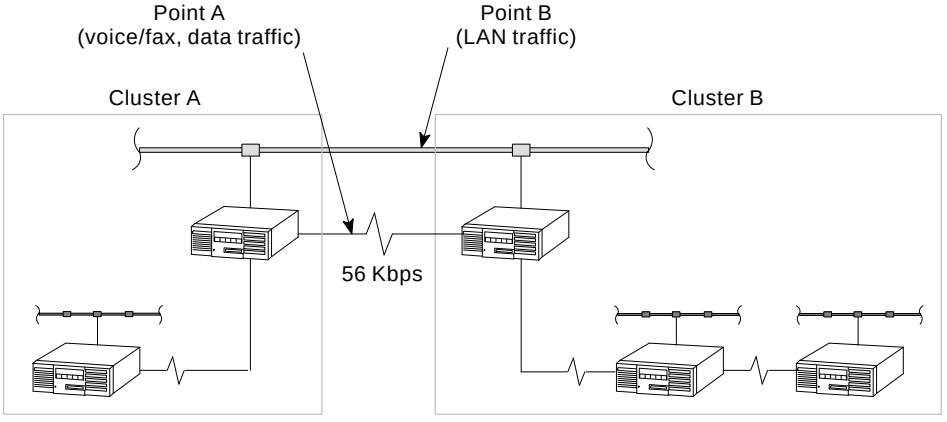
and enter the cluster name. The cluster name can be 1 – 15 alphanumeric characters long. If only one character is desired, it must be an alphabetic character. Then reset the unit to put the cluster name into effect.

Once a cluster name has been defined, the node will only communicate with other nodes (up to 11) having the same cluster name. An Integration Router's assigned cluster name appears when you execute a LIST BRIDGE STATUS command as described on page 7-19.

Communicating Between Clusters

Clusters increase network efficiency by separating LAN traffic from voice/fax and data traffic.

As an example, refer to the figure below. Though the two clusters shown are connected through a 56 Kbps WAN network link (point A), the link only carries voice/fax and data traffic. LAN traffic between the clusters passes through the common LAN at point B. Once inside a particular cluster, LAN traffic is then forwarded over the WAN links of the particular cluster. Connecting clusters in this manner increases overall network performance and adds additional network security, as nodes in a particular cluster may be set to forward or accept only certain packet types (filtering).



Cluster-to-Cluster Communication

Filtering (point-to-point and multi-site applications)

This section describes the filtering capabilities and the types of filters offered by the Integration Router. Filters instruct the Integration Router whether to ignore or accept specific types of packets. This may be based on protocol, hardware address, pattern, and source information.

Every node on a LAN segment sees every packet traveling to and from every other node on that segment. As more nodes are added to the segment, traffic increases, and with it collisions, resulting in slower communication.

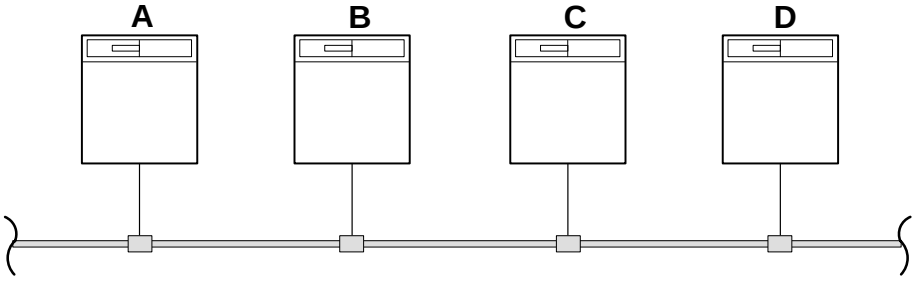
A key function of a bridge/router is to isolate network traffic. In so doing, the bridge/router can control (filter) the amount of traffic traveling between segments, reducing the overall network traffic.

For more information on specific filtering commands, refer to Section 7, Command Reference.

Destination Address Filtering

The Integration Router automatically provides destination address filtering by passively monitoring traffic on the local LANs. Only packets destined for an interconnected LAN are forwarded across the WAN link. Packets not destined for another LAN segment are considered local and ignored (filtered). As the Integration Router *listens* to network traffic, it learns which nodes and devices are located on the local LAN, and uses this information to ignore or forward traffic across the WAN. Therefore, any given segment carries only traffic to and from devices or nodes on that segment. This isolation reduces network traffic.

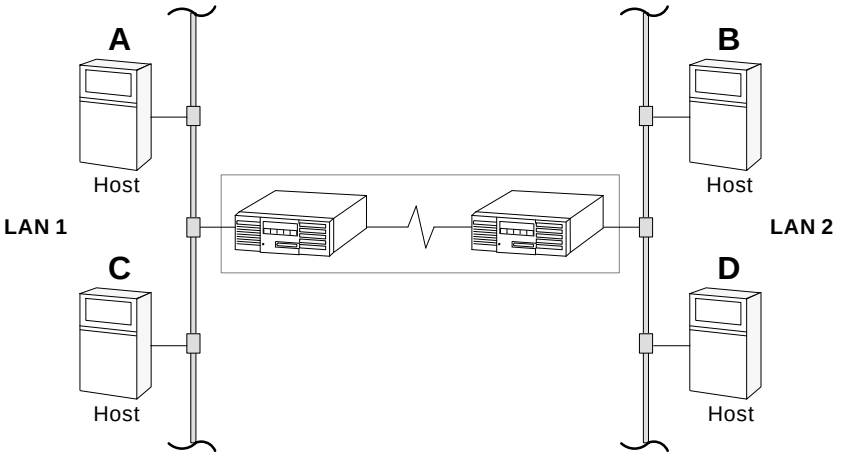
The figure shows a LAN segment with four hosts connected. As an example, hosts A and C send 20 packets per second to each other, as do B and D. In addition, each host sends two packets per second to each of the other three hosts. The total traffic within this segment is 104 packets per second (2x20 + 2x20 + 2x3x4).



Four Hosts Connected to the Same LAN Segment

In order to reduce traffic, the original segment can be divided into two smaller segments labeled LAN 1 and LAN 2, and connected via two units and a WAN link. LAN 1 only carries traffic between hosts A and C, and any packets crossing the link. The same is true for LAN 2; carrying only traffic between hosts B and D and any packets crossing the WAN link (shown in the next figure).

The local Integration Router monitors each LAN and only allows packets to pass that are destined for the opposite LAN; packets between hosts (or devices) of the same LAN are discarded. The amount of traffic within each segment is reduced to 56 (2 x 20 + 16).



Divided LAN Segments

Address Tables

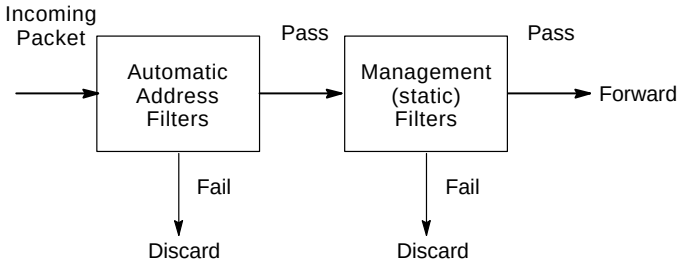
In order to perform automatic destination address filtering, each Integration Router on the network maintains a table of addresses for devices connected to the local LAN and Integration Routers/RLBs in the same cluster. When receiving a packet, the Integration Router consults the address table to determine if the packet should be forwarded across the WAN or discarded (remain on the local LAN). Not only does the Integration Router check the packet's destination address, but it also looks at the source address to learn (or confirm) which LAN segment the sending node or device is attached to, making certain packets are not routed back to their source node or device.

There are three types of address categories maintained in the address table: permanent, static, and dynamic.

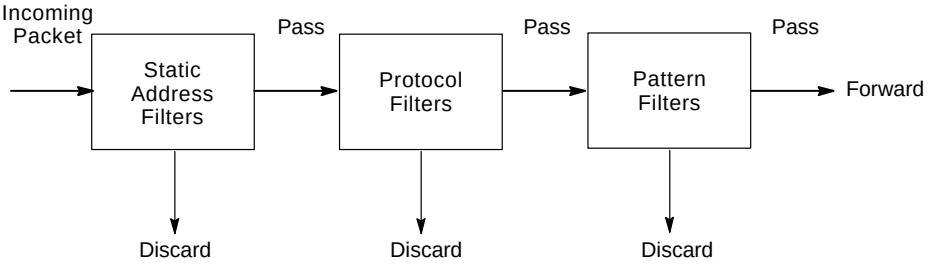
- **Permanent** entries are reserved addresses and cannot be removed from the table.
- **Static addresses** are address filters entered by management action, as described below.
- **Dynamic addresses** are compiled as the Integration Router monitors network traffic. Each time a new node or device transmits, its source address is added to the database. At the same time, nodes or devices that have not been heard from in a specified time are weeded out of the database.

Management Filters

In addition to destination address filtering, performed automatically by the Integration Router, network administrators can specify other filters such as static address filters, protocol filters, and pattern filters. These filters take effect only after a packet has passed the destination address filter.



Automatic and Management (Static) Filtering



Management Filter Details

Filter Diagram

Static Address Filters

Static address filters force packets matching either the source or destination address to be discarded, preventing traffic from individual hosts from crossing the WAN. An Ethernet address, also referred to as a hardware address, is a 6-byte value expressed in hexadecimal, in the form xx-xx-xx-xx-xx-xx, where x is a hexadecimal digit ranging from 0-9 or A-F. Devices from a particular manufacturer generally begin with the same first three address bytes. For example, MICOM's hardware addresses are 00-40-C5-xx-xx-xx. The hardware address is printed on the device. For MICOM equipment, the hardware address is printed on the back of the LAN module.

Protocol Filters

If configured, packets with an Ethernet-level protocol that matches the configured protocol are discarded. Ethernet protocols have a 2-byte value, and may be specified either by name or number.

The offset for Ethernet_II frames is 0x0c.
The offset for Ethernet_SNAP is 0x12.

Pattern Filters

Pattern filters consist of a pattern and an offset (n). All packets in which the *nth* byte matches the specified pattern will be discarded, regardless of address or protocol.

Exclusively Operating Filters

Any of the filters configured by the network managers can be made to operate in the exclusive mode. When the filter is in an exclusive mode, packets that match the filter parameters are forwarded, and all others are discarded. This contrasts with the default, non-exclusive operating mode, where packets that match the filter parameters are discarded.

To enable or disable filters, refer to Section 7, Command Reference.

RARP Protocol Filtering

RARP packets cannot be filtered using protocol filters (i.e., `SET BRIDGE GLOBAL PROTOCOL RARP ADD`). In order to filter RARP packets, you must use pattern filtering (i.e., `SET BRIDGE GLOBAL PATTERN 0x8035 0x0C ADD`).

The Spanning Tree

The spanning tree eliminates data loops in a bridged network (or, rather, protocols that are bridged) by making certain only one path exists between any two nodes in the network. This prevents multiple transmission of packets onto network segments by disabling redundant connections to each segment, usually by disabling one or more bridge ports. Without the spanning tree, packets could endlessly propagate around the network loop.

Organization

In a network of multiple bridges, one bridge is selected by algorithm to serve as the root bridge. The other bridges are either active branches extending from the root bridge or are in a passive, backup state. Those in a backup state do not forward packets.

The command DEFINE BRIDGE SPAN (page 7-10) enables or disables the Integration Router's participation in the spanning tree. The default is enabled, and typically should not be changed.

Active or Passive

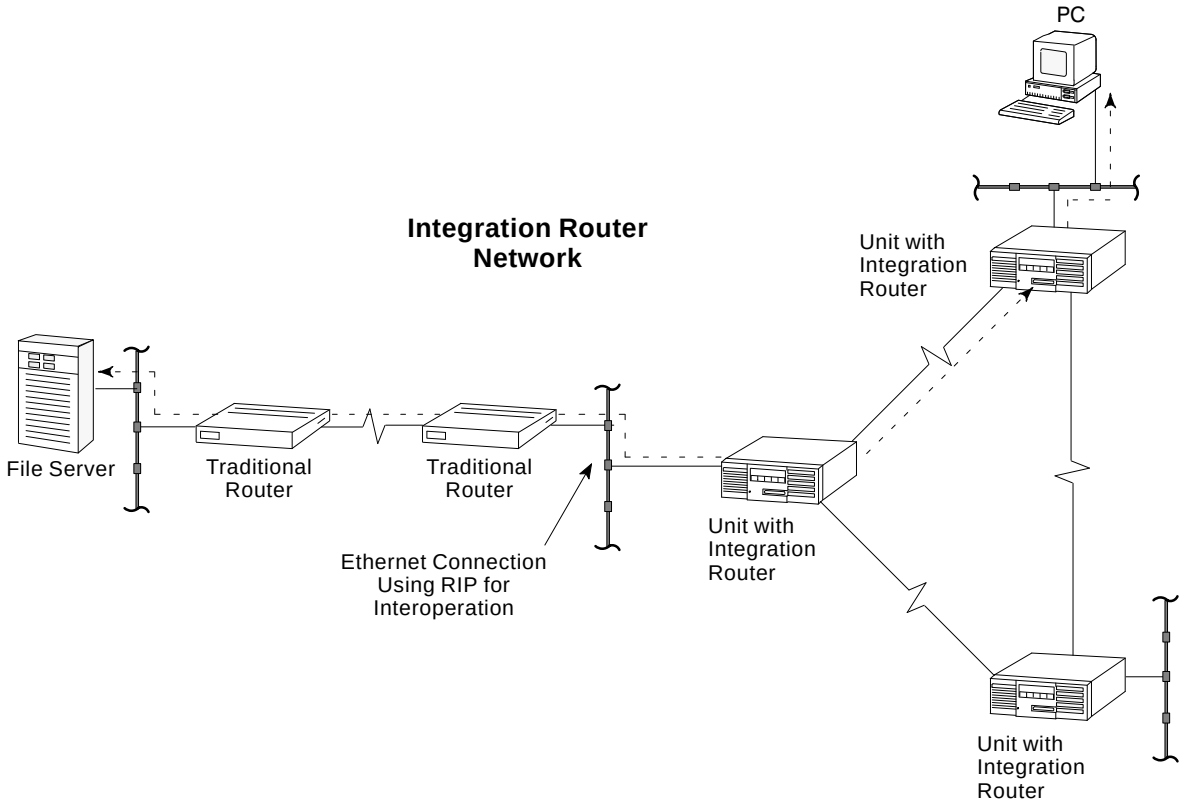
Upon power up, the bridges communicate with each other and decide who will be the root bridge, which bridge ports will be active, and which ports will be passive. The bridges use BPDU (Bridge Protocol Data Units) packets to communicate with each other. The propagation of BPDU packets allows the bridges to see loops and decide which bridge ports to disable. The network administrator can control which bridge ports will be active by setting certain parameters that are used in the spanning tree algorithm. These parameters are transmitted between bridges via the BPDU packets.

The root bridge will be the one with the lowest priority number. The priority number can be set by the network administrator to make sure one bridge is always the root bridge. Or, if the priorities are the same, the bridge with the lowest Ethernet address will be root.

The spanning tree algorithm determines the best path to forward packets based on root path cost, port priority, and bridge identifier (Ethernet address). All other redundant paths (loops) are disabled. The *Root Path Cost* is the total cost from the bridge that transmitted the BPDU configuration message to the bridge listed in the bridge identifier field of the BPDU packet. This is equivalent to the number of hops the configuration message made. The *Bridge Identifier* is the Ethernet address of the bridge that transmitted this BPDU packet along with that bridge's priority. The *Port Priority* is a numerical value that is assigned to each port. The lower the numerical value, the higher the priority. For example, a port assigned priority 64 has a higher priority than a port assigned priority 128.

Interoperation With Traditional Routers

The Integration Router interoperates with traditional routers, such as Cisco, 3Com, Bay Networks, etc. This is accomplished using the Router Information Protocol (RIP). The requirement for enabling this operation is that the traditional router must be on the same LAN segment as the Integration Router, as shown below. Also, the traditional router must use RIP and RIP must be enabled at the Integration Router. RIP is enabled at the Integration Router by default. See page 7-23 for the syntax of the command to enable/disable RIP at the Integration Router.



Management of the Integration Router

The Integration Router can be managed in the following ways:

- The unit's Command Facility provides direct access to the Integration Router's command line interface. Just select the menu item titled Integral LAN Local Mode Access. The Command Facility can be accessed via any asynchronous channel or via the Command Port, if an NMS module is installed. See the WAN documentation provided with your units for details about accessing the Command Facility.
- You can telnet into the Integration Router command line interface. The requirements to enable this function are:
  - You must define an IP address for the Integration Router. See page 7-39 for the command syntax to set the IP address.
  - Telnet connections must be enabled. See page 7-39 for the command syntax to enable telnet connections. By default, the Integration Router permits telnet connections to its command line interface.
- You can login to the Integration Router via the LAT network. To enable this access method, the requirements are:
  - You must assign a server name to the Integration Router. See page 7-41 for the command syntax to enter a server name.
  - LAT connections must be enabled. See page 7-39 for the command syntax to enable LAT connections. By default, the Integration Router permits LAT connections to its command line interface.
- You can use MICOM's NETMan network management program to access the Integration Router's command line interface. This is done by selecting **Emulation** and **Network** from the NETMan's Control Center Top Menu, then selecting the Integration Router Module from the Select Facility menu. See the NETMan User's Manual for details about this function.
- You can use off-the-shelf network management programs that use SNMP (Simple Network Management Protocol) to access certain information about the Integration Router. The Integration Router supports the GET (read) functions of MIB-II (Management Information Base) objects. See Appendix C for a list of the MIB objects supported. To enable the Integration Router to respond to SNMP queries, you must define an IP address for the Integration Router. See page 7-39 for the command syntax to set the IP address.

5 IP Routing

The Integration Router performs traditional IP routing in accordance with RFC 1009, *Requirements For Internet Gateways*.

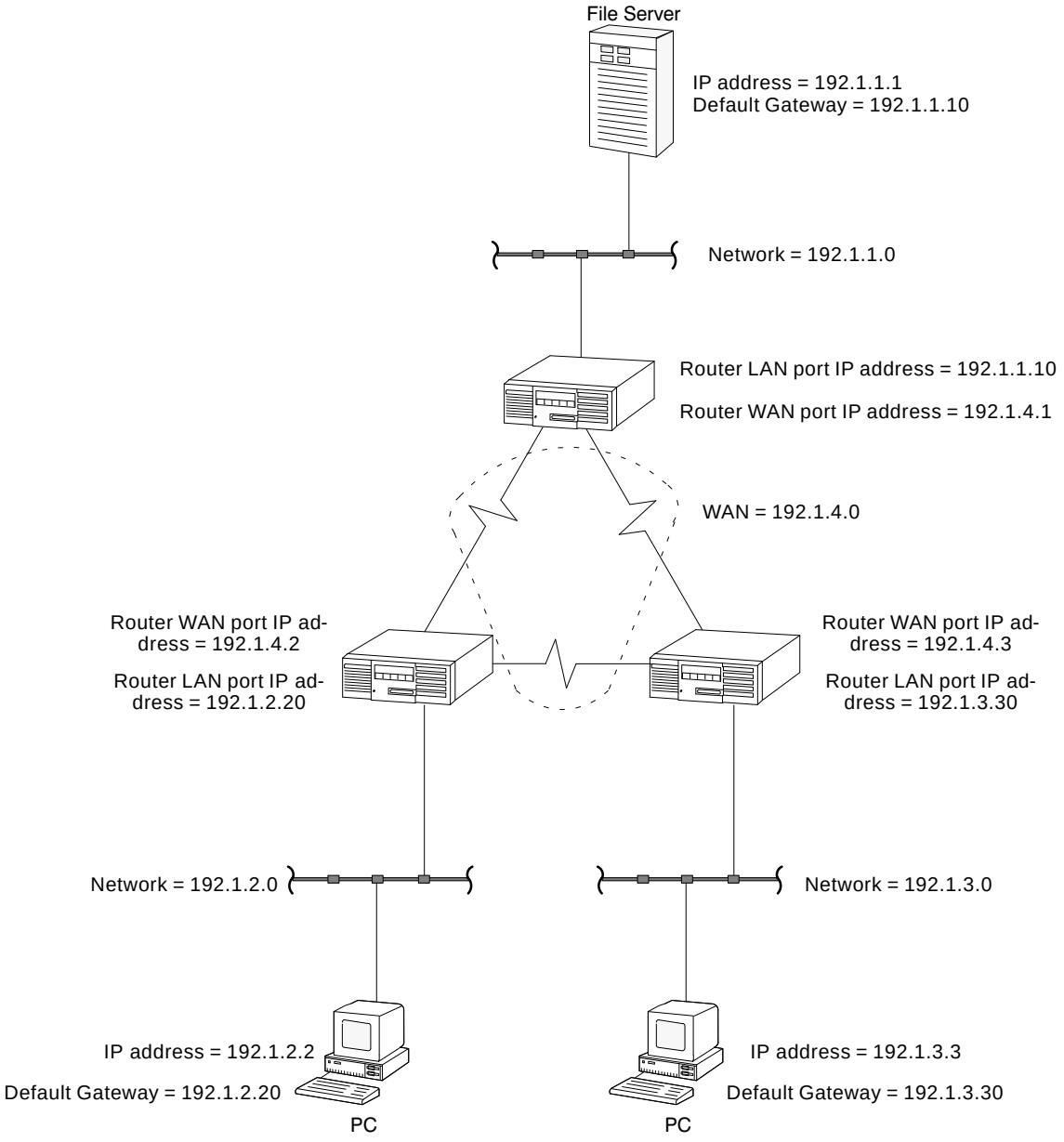
The determination of whether traditional routing is required for a network is beyond the scope of this manual. It is assumed that you are aware of the effects of routing on your LANs and that your network meets the addressing requirements for routing IP networks.

To permit traditional IP routing, the following network address requirements must be met:

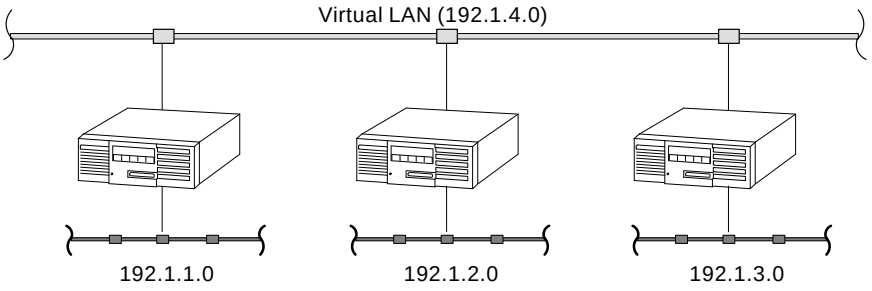
- Network addressing and subnetting:
  - You must have acquired the necessary IP addresses from the Internet Authority.
  - All LAN segments and all WANs must be assigned different network numbers.
  - All devices on the same WAN and in the same cluster must be configured with the same network number for their WAN interface. That is, the network number portion of the IP address must be the same for all devices on the WAN.
  - Devices in different WAN clusters must have different network numbers.
- Node addressing. You must assign unique IP addresses to all the devicies on your network. Specifically for the Integration Router:
  - The LAN port of each Integration Router must be assigned an IP address.
  - The WAN port of each Integration Router must be assigned an IP address. Only one IP address is required for the WAN port, no matter how many physical links the unit uses to access the WAN.
  - Since each LAN segment and each WAN must be assigned different network numbers, the network number portion of the IP addresses for the Integration Router's LAN port and its WAN port must be different.
  - You can define subnet masks for the IP addresses of both the Integration Router's LAN port and its WAN port. The default subnet masks are based on the classes of the IP addresses (i.e., class A, B, or C).
- Default gateway. There must be a default gateway (router) established for all PCs, workstations, servers, and other devices in the network. The devices forward to this gateway any packets that are addressed to a node that is unknown to them.

- Domain Name Servers (DNS). The DNS host tables must be updated to reflect the new network architecture established by routing.
- NFS file systems. It is not recommended that nodes mount NFS file systems of remote host systems (i.e., host systems located across the WAN).
- Bootp. Any machine that requires Bootp during startup must either be on the same LAN segment as the Bootp host, or the Bootp host must be able to download Bootp through the Integration Router.

The IP addressing requirements are illustrated in the example network diagram below.


File Server
IP address = 192.1.1.1
Default Gateway = 192.1.1.10
Network = 192.1.1.0
Router LAN port IP address = 192.1.1.10
Router WAN port IP address = 192.1.4.1
WAN = 192.1.4.0
Router WAN port IP address = 192.1.4.2
Router LAN port IP address = 192.1.2.20
Router WAN port IP address = 192.1.4.3
Router LAN port IP address = 192.1.3.30
Network = 192.1.2.0
Network = 192.1.3.0
IP address = 192.1.2.2
Default Gateway = 192.1.2.20
PC
IP address = 192.1.3.3
Default Gateway = 192.1.3.30
PC

From the Internet's point of view, the network architecture appears as follows:



The units appear to the Internet as routers, with the WAN considered as one virtual LAN.

To turn on IP routing, perform the following at each Integration Router:

1. Set the Integration Router's LAN port IP address. Enter the following at the Local> prompt:

   `DEFINE SERVER IPADDRESS ip_address`

   for example: *`define server ipaddress 192.1.1.10`*

   You can also assign a subnet mask to the Integration Router's LAN port IP address. At the Local> prompt, enter:

   `DEFINE SERVER SUBNET MASK mask`

   for example: *`define server subnet mask 255.255.255.0`*

   See page 7-43 for information about the subnet mask.

2. Set the Integration Router's WAN port IP address. Enter the following at the Local> prompt:

   `DEFINE IP WAN IPADDRESS ip_address`

   (where *ip_address* is the IP address for the Integration Router's WAN interface, for example: *`define ip wan ipaddress 192.1.4.1)`*

   You can also assign a subnet mask to the IP WAN address. At the Local> prompt, enter:

   `DEFINE IP WAN SUBNET mask`

   for example: *`define ip wan subnet 255.255.255.0`*

   See page 7-25 for information about the subnet mask.

3. Enable IP routing. At the Local> prompt, enter:

   `DEFINE IP ROUTING ENABLED`

4. Initialize the Integration Router to set the above parameters into effect and establish the routing operation. At the Local> prompt, enter:

   `INITIALIZE SERVER DELAY 0`

Note: It will take at least 5 minutes, after the Integration Router is reset, for the IP routing operation to get fully established.

IPX Routing 6

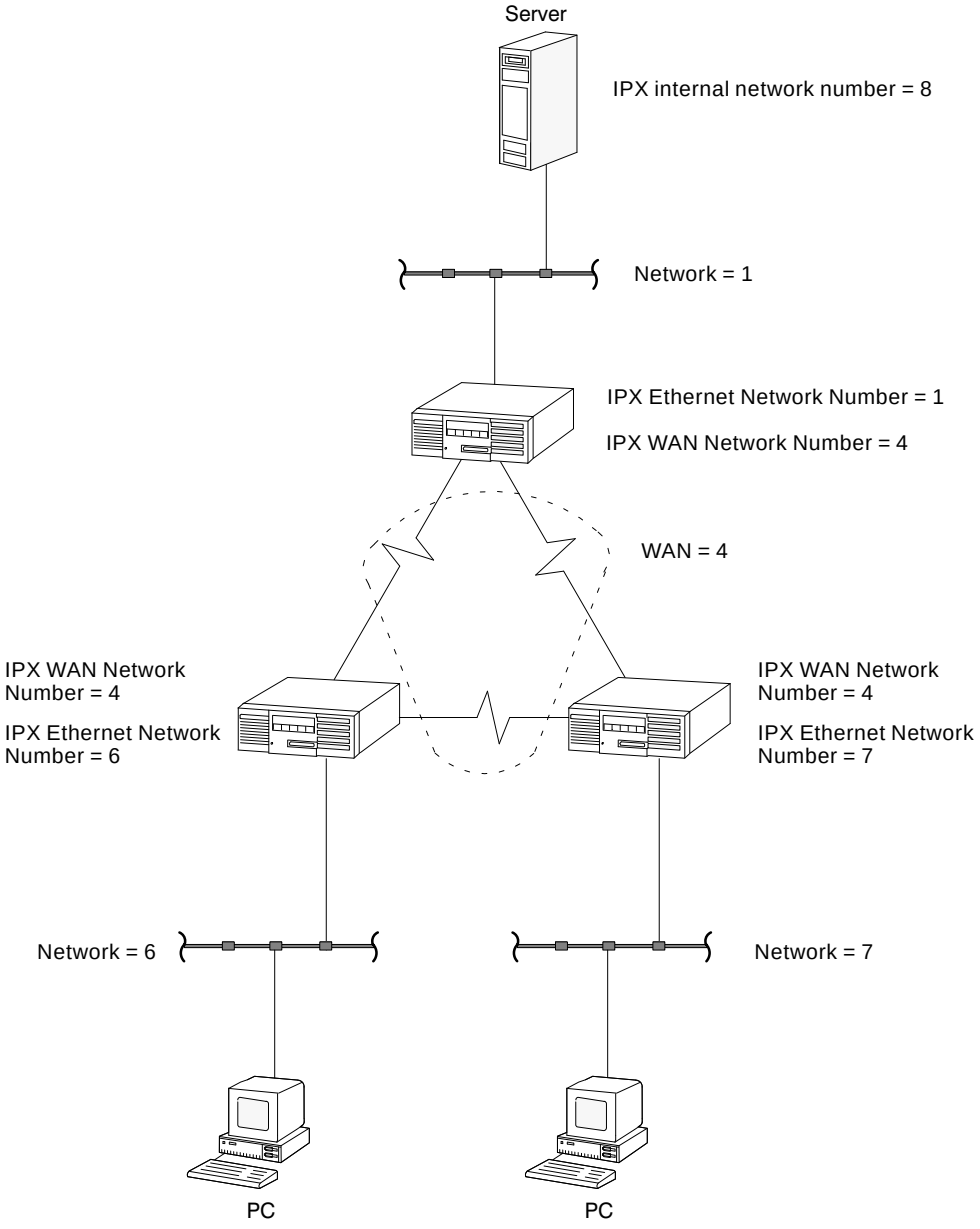
Traditional IPX routing provided by the Integration Router complies with *IPX Router Specification*, version 1.10, Novell part number 107-000029-001. The Integration Router also supports the delta update capability described in *Novell IPX Over Various WAN Media*, RFC 1362. Delta update optimizes available WAN bandwidth by sending only routing table and SAP table changes across the WAN, instead of periodically sending the entire tables. Delta update can be disabled, if desired.

The determination of whether traditional routing is required for a network is beyond the scope of this manual. It is assumed that you are aware of the effects of routing on your LANs and that your network meets the addressing requirements for routing IPX networks.

To permit traditional IPX routing, the following network address requirements must be met:

- Each LAN segment must be assigned an IPX network number. The network numbers for each LAN segment must be unique. In bridged IPX networks, all LAN segments have the same network number and thus are considered one virtual LAN segment. To route, however, each LAN segment must have its own network number.
- Each WAN must be assigned an IPX network number. The network number for each WAN must be unique. Only one network number is required for the WAN, no matter how many physical links the WAN consists of. The WAN for all nodes in one cluster is considered as one virtual LAN segment. Thus, all devices on the same WAN, and in the same cluster, must be configured with the same IPX network number for their WAN interface.
- Devices in different WAN clusters must have different network numbers for their WAN interface.
- All NetWare servers on a network segment must have unique internal network numbers. These numbers must not be the same as any LAN segment network number or WAN network number.
- IPX network numbers are in the range 1 to FFFFFFFE, hexadecimal.

The IPX addressing requirements are illustrated in the example network diagram below.


Server
IPX internal network number = 8
Network = 1
IPX Ethernet Network Number = 1
IPX WAN Network Number = 4
WAN = 4
IPX WAN Network Number = 4
IPX Ethernet Network Number = 6
IPX WAN Network Number = 4
IPX Ethernet Network Number = 7
Network = 6
Network = 7
PC
PC

To turn on IPX routing, perform the following at each Integration Router:

1. Enter the WAN network number and the LAN network number. At the Local> prompt, enter:

   ```
   DEFINE IPX WAN NETWORK number
   ```

   (where *number* is the WAN interface network number in hexadecimal/decimal)

   ```
   DEFINE IPX ETHERNET NETWORK number
   ```

   (where *number* is the LAN network number in hexadecimal/decimal)

2. Configure the IPX frame type to be utilized on the Integration Router's LAN interface (LAN port). At the Local> prompt, enter:

   ```
   DEFINE IPX ETHERNET FRAME_TYPE option
   ```

   (where *option* is the type of IPX frames to be used. The options are LLC, RAW, SNAP, and E2. The default is RAW.)

3. Turn on IPX routing. At the Local> prompt, enter:

   ```
   DEFINE IPX ROUTING ENABLED
   ```

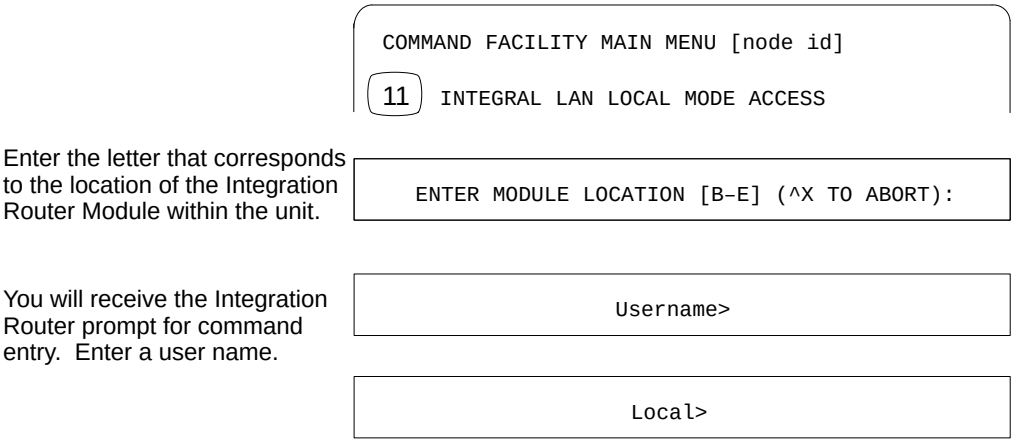
4. To put the above settings in effect and turn on IPX routing, the Integration Router must be reset. Enter the following command at the Local> prompt:

   ```
   INITIALIZE SERVER DELAY 0
   ```

Note: It will take at least 5 minutes, after the Integration Router is reset, for the IPX routing operation to get fully established.

Command Reference 7

The following are the commands available at the Local> prompt. To get the Local> prompt, proceed as follows:


COMMAND FACILITY MAIN MENU [node id]
11 INTEGRAL LAN LOCAL MODE ACCESS
Enter the letter that corresponds to the location of the Integration Router Module within the unit.
ENTER MODULE LOCATION [B–E] (^X TO ABORT):
You will receive the Integration Router prompt for command entry. Enter a user name.
Username>
Local>

Command Syntax

The commands are not case sensitive. Lower, upper, or mixed-case entries are treated identically. In addition, commands may be abbreviated by typing in only a few letters for each parameter in the command (for example, `SHOW BRIDGE STATUS` may be entered as `SH BR ST`). In some cases, only the first letter of each command is needed.

Command Reference Syntax

For the purpose of this manual, commands are listed in upper-case letters, while user defined parameters are shown in lower-case. For example, the command:

```
SET SERVER IPADDRESS ip_address
```

sets the Integration Router's IP address. SET SERVER IPADDRESS represents the command, while *ip_address* is the user defined parameter.

In cases where the user has an option between two commands, both commands are shown separated by a slash, though only one command is entered. For example:

```
SET/DEFINE BRIDGE MULTICAST ENABLED/DISABLED
```

is a sample command listing. When entered at the Local> prompt, use either SET **or** DEFINE; ENABLED **or** DISABLED as shown in the following examples.

```
Local> SET BRIDGE MULTICAST ENABLED
Local> DEFINE BRIDGE MULTICAST ENABLED
Local> SET BRIDGE MULTICAST DISABLED
```

Many commands are *privileged*. This means that to use these commands, you must be a privileged user. This is done by either:

- Accessing the Integration Router via the unit's Command Facility Main Menu (select the menu item called Integral LAN Local Mode Access).
- When accessing the Integration Router using telnet, enter the following commands at the Local> prompt:

  ```
  Local> SET PRIVILEGED
  Password> ######
  ```

  where ###### is the privileged user password (see page 7-42 for information on the privileged user password).

Organization

Commands are divided into several groups: Bridge Commands, IP Routing Commands, IPX Routing Commands, Server Commands, and General Commands. All commands are listed, in order, beginning on the following page.

Bridge Commands

Set/Define Commands

ARPBcast Filtering 7-5
ARPSpoof 7-6
ARPSpoof Blocking Thold 7-6
ARPSpoof Blocking Timer 7-6
ARPSpoof Cache_Timeout 7-7
Broadcast 7-7
Cluster 7-7
Compression 7-8
Multicast 7-8
SAPSpoof 7-9
SAPSpoof Blocking Thold 7-9
SAPSpoof Blocking Timer 7-9
Span 7-10
State 7-10
Weed 7-10

Filtering Commands

Exclusive 7-12
Address 7-12
Pattern 7-12
Protocol 7-12
Specific 7-12
Global 7-13
Address 7-13
Pattern 7-13
Protocol 7-13
Specific 7-14
Destination 7-14
Pattern 7-14
Protocol 7-14
Source 7-14

Show/Monitor/List Commands

Addresses 7-15
ARPBlock 7-15
ARPCache 7-16
Counters 7-16
Nodes 7-18
Status 7-19
Traffic 7-20

IP Routing Commands

Set/Define Commands

Exclusive Gateway 7-21
Exclusive Network 7-21
Filtering 7-22
Global Gateway 7-22
Global Network 7-23
RIP 7-23
Routing 7-23
Static 7-24
Static Default 7-24
WAN IPaddress 7-25
WAN Subnet Mask 7-25

Show/Monitor/List Commands

ARP 7-26
Counters 7-26
IP 7-27
Routes 7-27

IPX Routing Commands

Set/Define Commands

Ethernet Frame_Type 7-28
Ethernet Network Number 7-28
Exclusive Network 7-29
Exclusive SAP_Type 7-29
Filtering 7-29
Global Network 7-30
Global SAP_Type 7-31
Routing 7-32
WAN Network Number 7-32
WAN Optimize 7-33

Show/Monitor/List Commands

Counters 7-34
IPX 7-35
Routes 7-36
SAPs 7-36

Server Commands

Set/Define Commands

Announcements 7-37
Bootp 7-37
Circuit Timer 7-37
Domain 7-38
Ethernet 7-38
Identification 7-38
Incoming 7-39
Both 7-39
LAT 7-39
None 7-39
Nopassword 7-39
Password 7-39
TELNET 7-39
IPaddress 7-39
Loadhost 7-40
Lock 7-40
Login Password 7-40
Maintenance Password 7-40

Set/Define Commands (cont'd)
- Multicast Timer 7-41
- Name 7-41
- Nameserver 7-41
- Number 7-41
- Password Limit 7-42
- Privileged Password 7-42
- Prompt 7-42
- Retransmit Limit 7-43
- Software Path 7-43
- Subnet Mask 7-43

Show/Monitor/List Commands
- Characteristics 7-44
- Counters 7-45
- Status 7-48

General Commands
- CLS 7-49
- Connect WAN 7-49
- Finger 7-49
- Help 7-49
- Initialize Server 7-50
- LO 7-50
- Lock 7-50
- Logout 7-50
- Man 7-50
- Ping 7-51
- Purge Sysdump 7-51
- Save 7-51
- Set
  - Ports 7-52
  - Privileged 7-52
  - Privileged Override 7-52
  - Noprivileged 7-52
- Show/Monitor/List 7-53
  - Ports 7-53
  - Sysdump 7-54
  - Users 7-54
- Su 7-54
- Test 7-55
  - Loop 7-55
  - Port 7-55
- Unlock Port 7-55
- WAN 7-55
- Who 7-55
- Zero Counters 7-55

Bridge Commands

Set and Define

The following bridge commands are entered using either the SET or DEFINE command.

The SET command configures Integration Router characteristics without changing the configuration stored in nonvolatile memory. Though SET changes system parameters immediately, these changes are lost when the unit is reset, unless a SAVE BRIDGE/SERVER/IP/IPX command is executed after using SET. SET may be used to make certain your configuration does not interfere with Integration Router or network operation, or to configure parameters on a temporary basis.

The DEFINE command changes the configuration stored in nonvolatile memory, though the changes do not immediately affect the Integration Router operation. Once DEFINE commands are entered, a system reset makes the changes effective.

Note: You should not intermix SET and DEFINE commands when entering a sequence of commands. The SET commands may override the DEFINE commands after the Integration Router is reset. The proper sequence is:

1. Enter all SET commands first.
2. Enter a SAVE command (see page 7-51 for the command syntax) to store the SET commands into nonvolatile memory.
3. Enter the DEFINE commands.
4. Reset the Integration Router to put the configuration into effect.

ARPBcast Filtering

Enables or disables the filtering of unsolicited broadcast ARP responses.

Command: `SET/DEFINE BRIDGE ARPBCAST FILTERING ENABLED/DISABLED`

Privilege: Privileged Command

Default: Enabled

Example: `SET BRIDGE ARPBCAST FILTERING DISABLED`

ARPSpoof

Enables or disables the ARP spoofing feature. This software algorithm allows the Integration Router to intercept most ARP broadcasts and handle them locally. This reduces the amount of broadcast traffic forwarded across the WAN. ARPSpoof is DEFINED only — you must reset the Integration Router to enable or disable ARP spoofing. The setting of ARPSpoof is ignored when IP routing is turned on.

Command: `DEFINE BRIDGE ARPSPOOF ENABLED/DISABLED`

Privilege: Privileged Command

Default: Enabled

Example: `DEFINE BRIDGE ARPSPOOF DISABLED`

ARPSpoof Blocking Thold

Configures the maximum number of consecutive outstanding ARP requests per destination node. When this threshold has been reached, the Integration Router will start the Blocking Timer and begin blocking all additional ARP requests to that destination node until the node responds or until the ARP-Spoof Blocking Timer expires.

Command: `SET/DEFINE BRIDGE ARPSPOOF BLOCKING THOLD number`

where *number* is a value in the range 3 to 40, or 999 (if you set the threshold value to 999, ARP requests will not be blocked)

Privilege: Privileged Command

Default: 5

Example: `SET BRIDGE ARPSPOOF BLOCKING THOLD 10`

ARPSpoof Blocking Timer

Configures the maximum amount of time that ARP requests will be blocked to a destination node. The ARPSpoof Blocking Timer is started when the ARPSpoof Blocking Thold number is reached.

Command: `SET/DEFINE BRIDGE ARPSPOOF BLOCKING TIMER time`

where *time* is a number in the range 20 to 60 seconds

Privilege: Privileged Command

Default: 20 seconds

Example: `SET BRIDGE ARPSPOOF BLOCKING TIMER 45`

ARPSpoof Cache_Timeout

Configures the weed time for the ARP spoofing table. Entries in the table that are inactive for the time specified by the Cache Timeout will be purged to make room for active entries.

Command: `SET/DEFINE BRIDGE ARPSPOOF CACHE_TIMEOUT time`

where *time* is a number in the range 60 to 600 seconds

Privilege: Privileged Command

Default: 600 seconds

Example: `SET BRIDGE ARPSPOOF CACHE_TIMEOUT 300`

Broadcast

Enables/disables the forwarding of broadcast packets across the WAN. If disabled, broadcast packets, with the exception of ARP messages, are not forwarded across the WAN. The destination address of broadcast messages is FF-FF-FF-FF-FF-FF hexadecimal. If broadcasts are disabled, ARP broadcast packets are still processed according to the SET BRIDGE ARPSPOOF command, to allow address resolution for TCP/IP connections.

ARP broadcasts may be enabled/disabled with a SET/DEFINE BRIDGE GLOBAL PROTOCOL filter (see page 7-11).

Command: `SET/DEFINE BRIDGE BROADCAST ENABLE/DISABLE`

Privilege: Privileged Command

Default: Enabled

Cluster

Assigns the Integration Router to a specific cluster. The Integration Router will only communicate with up to 11 interconnected Integration Routers and RLBs with the same cluster name. Integration Routers and RLBs set to the default cluster NONE will connect to each other. Cluster names are DEFINED only – the Integration Router must be reset for the new name to take effect.

Command: `DEFINE BRIDGE CLUSTER clustername`

Privilege: Privileged Command

Default: None (as an assigned cluster name)

Compression

Specifies the type of data compression to use across the WAN. You can specify software, hardware, or no compression.

Hardware compression uses a dedicated processor for data compression and frees up the Integration Router's processor for LAN communications activities. Hardware compression can be used only when the local and the remote Integration Routers/RLBs are version 4.0 or later and both nodes have hardware compression turned on.

Software compression uses the Integration Router's processor to perform data compression. Software compression can be used with Integration Routers or with RLB version 3.0 or later.

Selecting disabled for the local Integration Router turns off compression for both local and remote nodes (regardless of what the compression setting is for the remote node).

If there are dissimilar settings for compression between local and the remote Integration Routers/RLBs, the least feature set rule applies. For example, if hardware compression is selected at one end, but software compression is selected at the other end, the Integration Routers/RLBs will use software compression.

Compression is DEFINED only – the Integration Router must be reset to change the compression settings.

Command: `DEFINE BRIDGE COMPRESSION SOFTWARE/HARDWARE/DISABLED`

Privilege: Privileged Command

Default: Hardware

Multicast

Enables or disables forwarding of multicast packets across the WAN.

Command: `SET/DEFINE BRIDGE MULTICAST ENABLED/DISABLED`

Privilege: Privileged Command

Default: Enabled

SAPSpoof

Enables or disables the SAP/RIP spoofing feature. This software algorithm allows the Integration Router to intercept most SAP and RIP broadcasts and handle them locally. This reduces the amount of broadcast traffic forwarded across the WAN. SAPSpoof is DEFINED only – you must reset the Integration Router to enable or disable SAP/RIP spoofing. The setting of SAPSpoof is ignored when IPX routing is turned on.

Command: `DEFINE BRIDGE SAPSPOOF ENABLED/DISABLED`

Privilege: Privileged Command

Default: Enabled

Example: `DEFINE BRIDGE SAPSPOOF DISABLED`

SAPSpoof Blocking Thold

Configures the maximum number of consecutive outstanding SAP requests for a particular service type and RIP requests per network number. When this threshold has been reached, the Integration Router will start the Blocking Timer and begin blocking all additional SAP and RIP requests until the service type or network is learned, or until the SAPSpoof Blocking Timer expires.

Command: `SET/DEFINE BRIDGE SAPSPOOF BLOCKING THOLD number`

where *number* is a value in the range 3 to 40, or 999 (if you set the threshold value to 999, the SAP and RIP requests will not be blocked)

Privilege: Privileged Command

Default: 5

Example: `SET BRIDGE SAPSPOOF BLOCKING THOLD 10`

SAPSpoof Blocking Timer

Configures the maximum amount of time that SAP or RIP requests will be blocked. The SAPSpoof Blocking Timer is started when the SAPSpoof Blocking Thold number is reached.

Command: `SET/DEFINE BRIDGE SAPSPOOF BLOCKING TIMER time`

where *time* is a number in the range 20 to 60 seconds

Privilege: Privileged Command

Default: 20 seconds

Example: `SET BRIDGE SAPSPOOF BLOCKING TIMER 45`

Span

Configures the Integration Router to participate in spanning tree decisions. If the spanning tree is disabled, the Integration Router will neither participate in the spanning tree algorithm nor generate spanning tree packets.

Status of the spanning tree is shown with the SHOW/LIST BRIDGE command.

Span is DEFINED only – you must reset the Integration Router to enable or disable the spanning tree function.

Command: `DEFINE BRIDGE SPAN ENABLED/DISABLED`

Privilege: Privileged Command

Default: Enabled

State

Setting the Integration Router's bridge state to DISABLED removes its port from the spanning tree. The Integration Router will no longer forward packets to other nodes, regardless of cluster name. Enabling the Integration Router's bridge state puts its port into a blocking state. Depending on network topology, the Integration Router may transition into a forwarding state.

The SHOW/LIST BRIDGE command shows the current bridging state.

Command: `SET/DEFINE BRIDGE STATE ENABLED/DISABLED`

Privilege: Privileged Command

Default: Enabled

Weed

Sets the weed time for entries in the address table. Time is specified in seconds. If a dynamic address does not make contact with the Integration Router within the specified time, it is removed from the database.

Command: `SET/DEFINE BRIDGE WEED weedtime`

where *weedtime* equals 10 - 10000 seconds maximum (approximately 2.5 hours)

Privilege: Privileged Command

Default: 300 seconds

Filtering (using SET/DEFINE)

A **global** filter applies one test parameter to all packets. Usually, when you add a global filter, the Integration Router will block to the WAN (not forward) all packets that match the global filter. The SET/DEFINE BRIDGE GLOBAL command is used to add or remove global filters to/from the Integration Router database. Global filters can individually be set to either the non-exclusive mode or the exclusive mode. In the non-exclusive mode (the default), all packets except the ones that match the filter are forwarded across the WAN. In exclusive mode, only those packets that match the filter are forwarded across the WAN. The exclusive mode for each global filter is enabled or disabled using the SET/DEFINE BRIDGE EXCLUSIVE command.

Here are two examples of global filters in exclusive mode:

```
SET BRIDGE EXCLUSIVE ADDRESS ENABLE
SET BRIDGE GLOBAL ADDRESS 00-58-24-3b-4d-07 ADD
```

The above command sequence would forward across the WAN only those packets matching the Ethernet address 00–58–24–3b–4d–07.

```
SET BRIDGE EXCLUSIVE PROTOCOL ENABLE
SET BRIDGE GLOBAL PROTOCOL LAT ADD
```

The above command sequence would forward across the WAN only LAT packets.

If both of the above command sequences were entered, the result would be the combination of the two global filters in exclusive mode. That is, only LAT packets matching address 00–58–24–3b–4d–07 would be forwarded across the WAN.

The **specific** filters work as a set to apply a collection of parameters to all packets. The SET/DEFINE BRIDGE SPECIFIC command is used to add (or remove) specific filters into (or from) the Integration Router's database. You can create a maximum of 8 specific filters. The specific filter set can be configured to either the non-exclusive mode or the exclusive mode. In non-exclusive mode (the default) packets that match the specific filter set are not forwarded across the WAN. In exclusive mode, only those packets that match the specific filter set are forwarded. The exclusive mode for the specific filter set is enabled or disabled using the SET/DEFINE BRIDGE EXCLUSIVE SPECIFIC command.

Here is an example of a non-exclusive specific filter:

```
SET BRIDGE SPECIFIC 4 PATTERN 0x17 0x23 ADD
```

The above command would block telnet packets from being forwarded across the WAN, but allow other IP packets to be forwarded. The telnet type is 0x17 and it is located at byte 0x23 within the packet.

Here is an example of an exclusive specific filter:

```
SET BRIDGE EXCLUSIVE SPECIFIC ENABLE
SET BRIDGE SPECIFIC 7 SOURCE 00-02-45-e3-72-90
 PROTOCOL IP ADD
```

The above command sequence allows only the machine specified by the Ethernet address to be able to access the remote LAN, and only using the IP protocol. Packets from all other machines and all packets from the specified machine that are not IP packets are blocked (not forwarded).

Exclusive

Enables or disables exclusive filtering for the specified filter type. When exclusive filtering is enabled, only packets with matching parameters are forwarded onto the WAN. Packets with non-matching parameters are blocked.

Command: `SET/DEFINE BRIDGE EXCLUSIVE option ENABLE/DISABLE`

where *option* is one of the options listed below.

Privilege: Privileged Command

Examples:
```
DEFINE BRIDGE EXCLUSIVE ADDRESS DISABLE
DEFINE BRIDGE EXCLUSIVE PATTERN ENABLE
DEFINE BRIDGE EXCLUSIVE PROTOCOL DISABLE
DEFINE BRIDGE EXCLUSIVE SPECIFIC ENABLE
```

Options: Address – Enables or disables exclusive global address filtering. If enabled, only packets with a source or destination address matching an address in the address filter list are forwarded. The address filter list is constructed and changed using the Global filter command.

Pattern – Enables or disables exclusive global pattern filtering. If enabled, only packets matching a pattern in the pattern filter list are forwarded. The pattern filter list is constructed and changed using the Global filter command.

Protocol – Enables or disables exclusive global protocol filtering. If enabled, only packets which match a protocol in the protocol filter list are forwarded across the WAN. The protocol filter list is constructed and changed using the Global filter command.

Specific – Enables or disables exclusive specific filtering. If enabled, only packets matching the specific filter set are forwarded.

Global

Use set/define global commands to either ADD or REMOVE global filters from the database. NONE clears all filters for the option listed in the command.

Command: `SET/DEFINE BRIDGE GLOBAL option [parameter] ADD/REMOVE/NONE`

where *option* equals one of the options listed below.

Privilege: Privileged Command

Examples:
```
DEFINE BRIDGE GLOBAL ADDRESS 00-58-24-3b-4d-07 ADD
DEFINE BRIDGE GLOBAL PATTERN 0x12** 0x25 REMOVE
DEFINE BRIDGE GLOBAL PROTOCOL lat ADD
DEFINE BRIDGE GLOBAL ADDRESS NONE (clears all address filters)
```

Options:

Address – Specifies an Ethernet address to add or remove from the address filter list. An address may be either a text name or hexadecimal address. The Integration Router will attempt to resolve text names from LAT/IP traffic.

Pattern – Specifies a bit pattern to add or remove from the pattern filter list. The bit pattern is specified as a two-byte pattern (four hexadecimal digits) and an offset, both in hexadecimal. An asterisk (*) may be used as a four-bit wild card, meaning to match any four bits. The first byte of the Ethernet header is offset 0.

Protocol – Specifies an Ethernet-layer protocol to add or remove from the protocol filter list. The protocol may be specified as a two-byte hexadecimal value or as one of the following protocol names: APPLE (AppleTalk over Ethernet), ARP, DECNET (DECnet Phase IV, DNA routing), IP, IPX (NetWare IPX), LAT, LAVC, MOPDL (DEC MOP dump/load assistance), MOPRC (DEC MOP remote console), SNMP (will block SNMP at both the Ethernet and IP levels), and XNS.

Specific

Specific filters are combinations of filters that may specify a destination address, source address, protocol, and a pattern. There are eight specific filter slots, numbered 0 - 7. For example, to block IP packets to HOST1, type:

```
SET BRIDGE SPECIFIC 4 DESTINATION host1 PROTOCOL ip ADD
```

where *4* identifies the filter slot number (range 0-7).

Command: `SET/DEFINE BRIDGE SPECIFIC number option [parameter] ADD/REMOVE/NONE`

Examples:

```
DEFINE BRIDGE SPECIFIC 3 DESTINATION 00-05-23-78-ed-12 ADD
SET BRIDGE SPECIFIC 5 PATTERN 0x45 0x12 PROTOCOL IP ADD
SET BRIDGE SPECIFIC 5 PROTOCOL LAT DESTINATION
   00-05-23-78-ed-12 ADD
DEFINE BRIDGE SPECIFIC 7 SOURCE 00-05-23-78-ed-12 ADD
DEFINE BRIDGE SPECIFIC NONE (clears all specific filter slots)
```

Options:

Destination – Specifies destination address for a specific filter. An address may be either a text name (if the address is resolvable) or the hexadecimal Ethernet address.

Pattern – Specifies a bit pattern for the specific filter. The bit pattern is specified as a two-byte pattern followed by an offset, both in hexadecimal. In the pattern example above, 0x45 is the pattern and 0x12 is the offset. An asterisk (*) may be used as a four-bit wild card meaning match any four bits. The first byte of an Ethernet header is offset 0.

Protocol – Specifies an Ethernet-layer protocol to add or remove from the specific filter list. The protocol may be specified as a two-byte hexadecimal value or as one of the following protocol names: APPLE, ARP, DECNET (DECnet Phase IV, DNA routing), IP, IPX (NetWare IPX), LAT, LAVC, MOPDL (DEC MOP dump/load assistance), MOPRC (DEC MOP remote console), SNMP (will block SNMP at both the Ethernet and IP levels), and XNS.

Source – Specifies the source address for the specific filter. An address can be either a text name or actual IP address.

Show, Monitor, and List

The SHOW/MONITOR/LIST commands display various fields describing the Integration Router's status.

SHOW commands are used to display the current settings and statistics.

MONITOR commands are the same as SHOW commands except information is continuously updated every three seconds. The display can be stopped by pressing any key. MONITOR is a privileged command.

LIST commands are used to display the characteristics stored in nonvolatile memory, which may or may not be the same as those currently set. For example, if you use the SET command to temporarily change certain parameters, the changes will not appear with the LIST command. Please note that the LIST command is not used with every option described below.

Addresses

Displays the addresses of the devices most recently contacting the Integration Router.

Command: `SHOW/MONITOR BRIDGE ADDRESSES`

Privilege: Privileged Command

```
Local> show bridge addresses

Most recent addresses heard from:

Node 2 (Local Lan):
00-00-c0-2f-1b-5e                     00-00-c0-c8-8b-8b
Node 0 (Remote Lan):
00-40-c5-10-00-06 = RTS_0040C5100006  00-40-c5-00-2e-dd = RTS_5a-C_75EB
Node 1 (Remote Lan):
00-40-c5-1f-ff-36 = ROUTER_NTR75EA    00-00-c0-c2-8b-8b
```

ARPBlock

Displays the contents of the ARP spoof blocking queue.

Command: `SHOW/MONITOR ARPBLOCK`

Privilege: `MONITOR ARPBLOCK` is a Privileged Command

Example: `SHOW ARPBLOCK`

```
Local> show arpblock

Arpspoof Block  Queue

IP ADDR             STATUS    AGE   UNACK CTR
192.53.1.21         BRIDGING   11      3
192.53.1.22         BLOCKING   15      6
```

ARPCache

Displays the contents of the ARP cache table.

Command: SHOW/MONITOR ARPCACHE

Privilege: MONITOR ARPCACHE is a Privileged Command

Example: SHOW ARPCACHE

```
Local> show arpcache

Arp Cache

IP ADDR                MAC ADDRESS     AGE/STATUS      PORT
192.53.139.233    00:40:C5:11:00:01         STATIC         0
192.53.139.235    00:AA:00:80:C5:11            120         0
```

Counters

Displays counters for the Integration Router's bridge mode activity.

Command: SHOW/MONITOR BRIDGE COUNTERS

```
Local_2> show bridge counters
Current Bridge Configuration              Cluster/Node          <None>:-3

     Nodes:             18                            Top Changes:      0

LAN: Rx Pkt:        135715                            Tx Packets:       0
     Rejected:      135715   Rx Broadcast:   21210    Tx Broadcast:     0
     Forwarded:          0   Rx Multicast:   15212    Tx Multicast:     0
     Recv Rate:     15/sec   NIC Missed:         0    Wan Lost:         0
     Pkts to Us:     36764   Pkts to Wan:        0    BPDUs on LAN:     0

WAN: Pkts to Us:         0   Pkts to Lan:        0    BPDUs From Wan:   0

Local: Lan Bytes:           0             Remote: Lan Bytes:           0
       Wan Bytes:           0                     Wan Bytes:           0
       Compression:        0%                     Compression:        0%
```

Where:

Nodes – number of network nodes sending or receiving packets.

Top Changes – number of spanning tree topology changes occurring since start-up.

LAN Parameters

Rx Pkt – number of packets from the LAN that the Integration Router looked at.

Rejected – number of packets not forwarded due to filtering.

Forwarded – number of packets looked at and forwarded; should be equal to Rx Pkt less packets that were rejected.

Recv Rate – estimate of packet receive rate (expressed in packets/second).

Pkts to Us – packets that the Integration Router interpreted (broadcasts, multicasts, or packets with the Integration Router as a destination).

Rx Broadcast – number of broadcast packets seen by the Integration Router.

Rx Multicast – number of multicasts seen by the Integration Router.

NIC Missed – number of packets the Integration Router missed due to speed constraints.

Pkts to WAN – number of packets forwarded onto the WAN link.

Tx Packets – total number of packets transmitted by the Integration Router onto the LAN.

Tx Broadcast – number of broadcast packets transmitted by the Integration Router onto the LAN.

Tx Multicast – number of multicast packets transmitted by the Integration Router onto the LAN.

WAN Lost – number of packets dropped due to WAN link congestion.

BPDUs on LAN – number of BPDUs (bridge spanning tree packets) sent by the Integration Router.

WAN Parameters

Pkts to Us – number of packets received from a remote node that were destined for the Integration Router (broadcasts/multicasts, direct traffic, etc.).

Pkts to LAN – number of packets received from a remote node to be forwarded onto the LAN.

BPDUs from WAN – number of BPDUs (bridge spanning tree packets) sent to the Integration Router by a remote node.

Local/Remote Parameters

LAN Bytes – total number of bytes obtained from the LAN.

WAN Bytes – total number of bytes obtained from the WAN.

Compression – ratio of WAN bytes/LAN bytes received; a 10% compression ratio indicates that there is a 10% savings in data transmission.

Nodes

Displays information regarding active Integration Routers/RLBs in the cluster.

Command: SHOW/MONITOR BRIDGE NODES

```
Local> show bridge nodes
Current Bridge Configuration              Cluster/Node                 <None>:0
   Hello Time:        2  Forward Delay Time:    15        Weed Time:        300
   Lan State:   Forward  Maximum Age:           24        Path Cost:          0

                ID/                                          Chan/       Pkt           Link
This node       Comp  H/W addr   CCM name  Bridge Name          State      To/Fr        Uptime
                00/H  00-04-C5   TPNET     RTS_0040C5000000     NA/FO        0/0        12d20h
                Active Nodes:
                01/H  00-04-22   TP        RTS_0040C5000422    01/FO    54784/54961      12d20h
```

Where:

Hello Time – time between bridge keepalive messages.

Forward Delay Time – time between port state transitions.

Weed Time – aging time for dynamic entries in the address database.

LAN State – current Integration Router port state.

Maximum Age – root bridge time-out duration.

Path Cost – port path cost through this node.

This Node – local Integration Router information.

Active Nodes – remote nodes connected to the local Integration Router.

ID/Comp – node number. This column also indicates the type of compression this node is equipped for (H = hardware, S = software).

H/W addr – hardware address of the node.

CCMname – node name of the CCM.

Bridge Name – Integration Router's or RLB's name.

Chan/State – CCM channel number/bridge state of remote node.

Pkt To/Fr – number of packets received/transmitted to/from a remote node.

Link Uptime – time the link has been active.

Status

Displays the Integration Router's current bridge and EasyRouter configuration, including active spanning tree parameters and filtering information.

Command: SHOW/MONITOR/LIST BRIDGE STATUS or SHOW/MONITOR/LIST BRIDGE

```
Local> show bridge status
Current Bridge Configuration                  Cluster/Node       <None>:0
   Hello Time:       2     Forward Delay Time:   15     Weed Time:    300
   Lan State:  Forward     Maximum Age:          24     Path Cost:      0

Root Bridge: 0x8000, 00-40-c5-00-00-00 ,-1  Spanning tree: Enabled

Global Characteristics: Broadcasts  Multicasts  Compression

Arp Spoofing                                    enabled
Arp cache timeout                               600
ArpSpoof block timeout                          20
ArpSpoof block threshold                        5
Bridging of unsolicited arp responses           enabled

Ipx RIP & SAP Spoofing                          enabled
SapSpoof block timeout                          20
SapSpoof block threshold                        5

Global Address Filters:                         None.
Global Protocol Filters:                        None.
Global Pattern Filters:                         None.
Specific Filters:                               None.
```

Where:

Hello Time – time between bridge keepalive messages.

Forward Delay Time – time between port state transitions.

Weed Time – aging time for dynamic entries in the address database.

LAN State – current Integration Router port state.

Maximum Age – root bridge time-out duration.

Path Cost – port path cost through this node.

Root Bridge – the hardware address and offset.

Spanning Tree – current state of the spanning tree.

Global Characteristics

Broadcasts – whether broadcasts are filtered or forwarded.

Multicasts – whether multicast is filtered or forwarded.

Compression – whether compression is enabled or disabled**.**

Arp Spoofing – whether ARP spoofing is enabled or disabled.

Arp cache timeout – the amount of time after which inactive entries in the ARP table are weeded out.

ArpSpoof block timeout – the maximum amount of time that ARP requests are blocked to a destination node.

ArpSpoof block threshold – the maximum number of consecutive outstanding ARP requests per destination node.

Bridging of unsolicited arp responses – whether filtering of unsolicited broadcast ARP responses is enabled or disabled.

Ipx RIP & SAP Spoofing – whether SAP/RIP spoofing is enabled or disabled.

SapSpoof block timeout – the maximum amount of time that SAP/RIP requests are blocked.

SapSpoof block threshold – the maximum number of consecutive outstanding SAP/RIP requests per service type/network number.

Global Address Filters – currently set/defined global address filters.

Global Protocol Filters – currently set/defined global protocol filters.

Global Pattern Filters – currently set/defined global pattern filters.

Specific Filters – number, type, and parameters for set/defined specific filters.

Traffic

Displays bridge traffic statistics categorized by packet protocol and size.

Command: `SHOW/MONITOR BRIDGE TRAFFIC`

Privilege: Privileged Command (if Monitor)

```
Local> show bridge traffic
             Packet lengths                          Packet types
          To Remote  From Remote                  To Remote  From Remote
L <  128      16002        16164             Tcp          0            0
L <  512      38946        38963             Udp          0            0
L <  768          0            0        Other Ip          0            0
L < 1024          0            0             Ipx          0            0
L < 1515          0            0             Lat      37090        37107
L >=1515          0            0      All Others      17858        18020
```

IP Routing Commands

Set and Define

For a description of the SET and DEFINE commands, please see *Bridge Commands*, page 7-5.

Exclusive Gateway

Enables or disables Exclusive Gateway filtering. If Exclusive Gateway filtering is enabled, only RIP broadcasts from gateways specified by the Global Gateway filters will be learned. The Global Gateway filters are applied to RIP broadcasts that arrive at the Integration Router from both its LAN port and from the WAN. Exclusive Gateway is DEFINED only. The Integration Router must be reset to enable or disable Exclusive Gateway filtering.

Command: `DEFINE IP EXCLUSIVE GATEWAY ENABLE/DISABLE`

Privilege: Privileged Command

Default: Disabled

Example: `DEFINE IP EXCLUSIVE GATEWAY ENABLE`

Exclusive Network

Enables or disables Exclusive Network filtering. If Exclusive Network filtering is enabled, only networks specified by the Global Network filters will be learned. The Global Network filters are applied to the Integration Router's LAN port and its WAN port. Exclusive Network is DEFINED only. The Integration Router must be reset to enable or disable Exclusive Network filtering.

Command: `DEFINE IP EXCLUSIVE NETWORK ENABLE/DISABLE`

Privilege: Privileged Command

Default: Disabled

Example: `DEFINE IP EXCLUSIVE NETWORK ENABLE`

Filtering

Enables or disables IP RIP filtering. The Integration Router can filter specific networks or gateway RIP broadcasts. Filtering a network or gateway RIP broadcast disallows that network or gateway from being learned by the Integration Router.

The filters are entered using the DEFINE IP GLOBAL GATEWAY and DEFINE IP GLOBAL NETWORK commands. IP RIP filtering is DEFINED only. The Integration router must be reset to enable or disable IP RIP filtering.

Command: `DEFINE IP FILTERING ENABLE/DISABLE`

Privilege: Privileged Command

Default: Disable

Example: `DEFINE IP FILTERING ENABLE`

Global Gateway

Adds or removes Global Gateway filters into the database. Normally, adding a Global Gateway filter to the database and enabling IP RIP filtering will block RIP broadcasts from that gateway from being learned by the Integration Router. If Exclusive Gateway filtering is enabled, only RIP broadcasts from that gateway will be learned. Global Gateway filters are applied to RIP broadcasts that arrive at the Integration Router from both its LAN port and from the WAN.

ADD puts the filter into the database. REMOVE deletes the filter from the database. NONE deletes all Global Gateway filters. You can enter a maximum of 16 Global Gateway filters.

Global Gateway is DEFINED only. The Integration Router must be reset to add or remove Global Gateway filters from the database.

Command: `DEFINE IP GLOBAL GATEWAY address ADD/REMOVE/NONE`

where address is the network number of the gateway in decimal, delimited by periods

Privilege: Privileged Command

Examples: `DEFINE IP GLOBAL GATEWAY 199.30.17.1 ADD`
Blocks all RIP broadcasts from gateway 199.30.17.1 from being learned by the Integration Router.

`DEFINE IP GLOBAL GATEWAY 199.30.17.1 REMOVE`
Removes the filter added above.

`DEFINE IP GLOBAL GATEWAY NONE`
Deletes all Global Gateway filters.

Global Network

Adds or removes Global Network filters into the database. Normally, adding a Global Network filter to the database and enabling IP RIP filtering will prevent the Integration Router from learning that network – whether that network is accessed via the LAN port or the WAN. If Exclusive Network filtering is enabled, only that network will be learned.

ADD puts the filter into the database. REMOVE deletes the filter from the database. NONE deletes all Global Network filters. You can enter a maximum of 16 Global Network filters.

Global Network is DEFINED only. The Integration Router must be reset to add or remove Global Network filters from the database.

Command: `DEFINE IP GLOBAL NETWORK number ADD/REMOVE/NONE`

where *number* is the network number in decimal, delimited by periods

Privilege: Privileged Command

Examples: `DEFINE IP GLOBAL NETWORK 199.30.17.0 ADD`
The Integration Router will not learn network 199.30.17.0, either from the WAN or from the Integration Router's LAN port.

`DEFINE IP GLOBAL NETWORK 199.30.17.0 REMOVE`
Removes the filter added above.

`DEFINE IP GLOBAL NETWORK NONE`
Deletes all Global Network filters.

RIP

Enables or disables the Integration Router's generation of Routing Information Protocol (RIP) packets to other routers.

Command: `SET/DEFINE IP RIP ENABLED/DISABLED`

Privilege: Privileged Command

Default: Enabled

Examples: `SET IP RIP DISABLED`

Routing

Enables or disables IP packet routing. Before IP packet routing can be enabled, IP addresses must be assigned for each Integration Router and for the WAN. IP routing is DEFINED only — the Integration Router must be reset to enable or disable IP routing

Command: `DEFINE IP ROUTING ENABLED/DISABLED`

Privilege: Privileged Command

Default: Disabled

Example: `DEFINE IP ROUTING ENABLED`

Static

Adds or removes static routes. A static route allows you to control how packets addressed to a particular host or network are to be routed. Static routes override the dynamic routing normally done by IP routers.

Command:
```
SET/DEFINE IP STATIC destination netmask gateway metric ADD
SET/DEFINE IP STATIC destination gateway REMOVE
SET/DEFINE IP STATIC NONE
```

Privilege: Privileged Command

Options: Destination – The IP address of a destination network or host whose packets are to be routed by this static route.

Netmask – The subnet mask for the destination.

Gateway – The IP address of the next hop (router).

Metric – The number of hops to the destination.

Default: None

Examples:
```
SET IP STATIC 192.53.139.000 255.255.255.0 192.73.220.70 2 ADD
```
(adds the static route)

```
SET IP STATIC 192.53.139.000 192.73.220.70 REMOVE
```
(removes the static route)

```
SET IP STATIC NONE
```
(removes all static routes)

Static Default

Adds or removes the default route. Any packets addressed to a destination for which the router has no known route will be forwarded to this gateway.

Command:
```
SET/DEFINE IP STATIC DEFAULT gateway/NONE
```

Privilege: Privileged Command

Options: Gateway – The IP address of the default router. This router must be on the same network as the Integration Router being configured (i.e., the same network number).

Default: None

Examples:
```
SET IP STATIC DEFAULT 192.53.139.70
```
(the default route is 192.53.139.70)

```
SET IP STATIC DEFAULT NONE
```
(deletes the default route)

WAN IPaddress

Assigns an IP address to the WAN interface. You need to define only one IP address, no matter how many physical links the WAN interface consists of. All devices on the same WAN and in the same cluster must be configured with the same IP network number (which is part of the IP address) for their WAN interface. Devices in different clusters must have different IP addresses configured for their WAN interfaces, as must devices on different WANs. WAN IPaddress is DEFINED only; you must reset the Integration Router to put the new address into effect.

Command: `DEFINE IP WAN IPADDRESS address`

where *address* = an IP address

Privilege: Privileged Command

Default: None

Example: `DEFINE IP WAN IPADDRESS 192.53.139.70`

WAN Subnet Mask

Sets an IP address subnet mask for the WAN interface. A mask will be set by default according to the IP WAN address. The mask is applied to target IP addresses to determine whether the destination address is on the WAN or not.

Command: `SET/DEFINE IP WAN SUBNET mask`

where *mask* is the subnet mask (for example, 255.255.255.0)

Privilege: Privileged Command

Default: Based on IP address that has been assigned for the WAN interface.

Example: `DEFINE IP WAN SUBNET 255.255.255.0`

Show, Monitor, and List

For a description of the SHOW, MONITOR, and LIST commands, please see *Show, Monitor, List Bridge Commands*, page 7-15.

ARP

Displays the contents of the ARP cache. All entries are dynamically learned. You cannot make changes to the parameters displayed in this table.

Command: `SHOW/MONITOR IP ARP`

Privilege: `MONITOR IP ARP` is a privileged command.

```
Local> show ip arp

    IP Address       Hardware Address   Type     Interface  RefCount
    192.1.7.6        00:40:c5:10:03:7d  Dynamic  wn0              26
    192.1.7.3        00:40:c5:00:2e:46  Dynamic  wn0               1
    192.1.7.2        00:40:c5:10:00:0a  Dynamic  wn0               1
    192.1.7.4        00:40:c5:00:10:96  Dynamic  wn0               1
```

Counters

Displays IP level statistics. Use the `ZERO COUNTERS IP` command to reset the IP counters.

Command: `SHOW/MONITOR IP COUNTERS`

Privilege: `MONITOR IP COUNTERS` is a privileged command.

```
Local> show ip counters
       0 packets received.
       0 packets received with header errors.
       0 packets received with address errors.
       0 packets forwarded.
       0 packets received with unknown protocols.
       0 inbound packets discarded.
       0 packets delivered to upper layers.
       0 transmit requests.
       0 discarded transmit packets.
       0 outbound packets with no route.
       0 reassembly timeouts.
       0 reassemblies required.
       0 reassemblies that went OK.
       0 reassemblies that Failed.
       0 packets fragmented OK.
       0 fragmentations that failed.
       0 fragment packets created.
       0 route discards due to lack of memory.
      64 default ttl.
```

IP

Displays the IP forwarding and RIP status, static routes, the interfaces and corresponding information, such as names (LAN and WAN), IP addresses, subnet masks, and status. SHOW IP displays the current configuration in use. LIST IP displays the configuration stored in nonvolatile memory.

Command: SHOW/MONITOR/LIST IP

Privilege: MONITOR IP is a privileged command.

```
Local_2> show ip

    IP Router:      Enabled
    RIP:            Enabled


    Interface  IP Address       Netmask            MTU  Status
    ln0        192.53.139.211   255.255.255.0     1500      Up
    wn0        192.53.140.1     255.255.255.0     1500    Down
    lo0        127.0.0.1        255.255.255.255   1500      Up

    Filtering                          disabled
    Network Filters                    None.
    Gateway Filters                    None.
```

Routes

Displays the IP (RIP) routing table. This table consists of dynamically learned routes and the configured static routes.

Command: SHOW/MONITOR/LIST IP ROUTES

Privilege: MONITOR IP ROUTES is a privileged command.

```
Local> show ip routes

    Destination      Gateway          Interf./link  Status  Metric  Type
    192.1.1.0        192.1.1.10       ln0       0     Up       0  Static
    192.1.2.0        192.1.7.2        wn0       2     Up       1  175
    192.1.3.0        192.1.7.3        wn0       5     Up       1  151
    192.1.4.0        192.1.7.4        wn0       1     Up       1  158
    192.1.5.0        192.1.7.5        wn0       3     Up       1  168
    192.1.6.0        192.1.7.6        wn0       6     Up       1  163
    192.1.7.0        192.1.7.1        wn0       0     Up       0  Static
```

IPX Routing Commands

Set and Define

For a description of the SET and DEFINE commands, please see *Bridge Commands*, page 7-5.

Ethernet Frame_Type

The Integration Router can receive multiple IPX frame types. Ethernet Frame_Type specifies the type of IPX frames that the local Integration Router will generate. If local workstations are using different types of IPX frames, connectivity to remote workstations will be provided only for those local workstations whose IPX frame type matches the Ethernet Frame_Type configured for the local Integration Router. Ethernet Frame_Type is DEFINED only – the Integration Router must be reset to change the IPX frame type.

Command: `DEFINE IPX ETHERNET FRAME_TYPE type`

where *type* = LLC, RAW, SNAP, or E2

Privilege: Privileged Command

Type: RAW = Ethernet_802.3
LLC = Ethernet_802.2
SNAP = Ethernet_SNAP
E2 = Ethernet_II

Default: RAW

Example: `DEFINE IPX ETHERNET FRAME_TYPE LLC`

Ethernet Network Number

Assigns an IPX network number to the Integration Router's LAN port. IPX network numbers are 32 bits long and are expressed as a hexadecimal value within the Integration Router. The Ethernet network number is DEFINED only. The Integration Router must be reset for the number to take effect.

When entering network numbers in hexadecimal, you must add 0x to the number before entering it. Example 1: a000 should be entered 0xa000. Example 2: 1c should be entered 0x1c. If the 0x is omitted, the following message will be displayed:

```
%Error: Bad network number or already assigned to other port
```

Command: `DEFINE IPX ETHERNET NETWORK number`

where *number* = a hexadecimal value between 1 and FFFFFFFE
or, a decimal value between 1 and 4294967294

Privilege: Privileged Command

Default: None

Examples:
```
DEFINE IPX ETHERNET NETWORK 1
DEFINE IPX ETHERNET NETWORK 0X1C
DEF IPX ETH NET 26
DEF IPX ETH NET 0XA000
```

Exclusive Network

Enables or disables Exclusive Network filtering. If Exclusive Network filtering is enabled, only RIP advertisements specified by the Global Network filters will be accepted/learned. Exclusive Network is DEFINED only. The Integration Router must be reset to enable or disable Exclusive Network filtering.

Command: `DEFINE IPX EXCLUSIVE NETWORK ENABLE/DISABLE`

Privilege: Privileged Command

Default: Disabled

Example: `DEFINE IPX EXCLUSIVE NETWORK ENABLE`

Exclusive SAP_Type

Enables or disables Exclusive SAP_Type filtering. If Exclusive SAP_Type filtering is enabled, only SAP advertisements specified by the Global SAP_Type filters will be accepted. Exclusive SAP_Type is DEFINED only. The Integration Router must be reset to enable or disable Exclusive SAP_Type filtering.

Command: `DEFINE IPX EXCLUSIVE SAP_TYPE ENABLE/DISABLE`

Privilege: Privileged Command

Default: Disabled

Example: `DEFINE IPX EXCLUSIVE SAP_TYPE ENABLE`

Filtering

Enables or disables SAP (service advertisement) and RIP (network advertisement) filtering. The Integration Router can filter specific SAP and RIP advertisements. Filtering a SAP or RIP advertisement from being accepted disallows that service or network from being accessed by devices. Example applications of SAP and RIP filtering are provided in Appendix D.

The filters are entered using the DEFINE IPX GLOBAL SAP_TYPE and DEFINE IPX GLOBAL NETWORK commands. IPX Filtering is DEFINED only. The Integration Router must be reset to enable or disable IPX Filtering.

Command: `DEFINE IPX FILTERING ENABLE/DISABLE`

Privilege: Privileged Command

Default: Disable

Example: `DEFINE IPX FILTERING ENABLE`

Global Network

Adds or removes RIP network advertisement filters into the database. Normally, adding a network filter to the database and enabling IPX Filtering will block the advertisement of that network. If Exclusive Network filtering is enabled, only that network advertisement will be accepted. The filter can be applied to advertisements coming from the Integration Router's LAN port, or to advertisements coming from the WAN, or from both ports. An example application of network filtering is located in Appendix D.

ADD puts the filter into the database. REMOVE deletes the filter from the database. NONE deletes all network filters. You can enter a maximum of 16 network filters.

Global Network is DEFINED only. The Integration Router must be reset to add or remove network filters from the database.

Command: `DEFINE IPX GLOBAL NETWORK number [option] ADD/REMOVE/NONE`

where *number* is the network number in decimal or hexadecimal

Privilege: Privileged Command

Option: Port – the values are ETHERNET, WAN, and BOTH. The default (that is, port is not specified in the command string) is ETHERNET, which applies the filter to the Integration Router's LAN port.

Examples:

```
DEFINE IPX GLOBAL NETWORK 0xc5 PORT ETHERNET ADD
```
or,
```
DEFINE IPX GLOBAL NETWORK 0xc5 ADD
```
Blocks all RIP advertisements with the network number 0xc5 that come from the Integration Router's LAN port.

```
DEFINE IPX GLOBAL NETWORK 0xc5 PORT ETHERNET REMOVE
```
or,
```
DEFINE IPX GLOBAL NETWORK 0xc5 REMOVE
```
Removes the filter added above.

```
DEFINE IPX GLOBAL NETWORK 6 PORT WAN ADD
```
Blocks all RIP advertisements with the network number 6 that come from the WAN.

```
DEFINE IPX GLOBAL NETWORK 6 PORT WAN REMOVE
```
Removes the filter added above. In this case, DEFINE IPX GLOBAL NETWORK 6 REMOVE would not work – the port must be specified.

```
DEFINE IPX GLOBAL NETWORK NONE
```
Deletes all Global Network filters.

Global SAP_Type

Adds or removes SAP service advertisement filters into the database. Normally, adding a SAP_Type filter to the database and enabling IPX Filtering will block the advertisement of the specified service. If Exclusive SAP_Type filtering is enabled, only that service advertisement will be accepted. The filter can be applied to advertisements coming from the Integration Router's LAN port, or to advertisements coming from the WAN, or from both ports. An example application of SAP_Type filtering is located in Appendix D.

ADD puts the filter into the database. REMOVE deletes the filter from the database. NONE deletes all SAP_Type filters. You can enter a maximum of 16 SAP_Type filters.

Global SAP_Type is DEFINED only. The Integration Router must be reset to add or remove SAP_Type filters from the database.

Command: `DEFINE IPX GLOBAL SAP_TYPE type [option] ADD/REMOVE/NONE`

where *type* is the service number in hexadecimal. The service number can be a maximum of four digits. Wild card characters are accepted.

Privilege: Privileged Command

Option: Port – the values are ETHERNET, WAN, and BOTH. The default (that is, port is not specified) is ETHERNET, which applies the filter to the Integration Router's LAN port.

Examples:

```
DEFINE IPX GLOBAL SAP_TYPE 4 PORT ETHERNET ADD
```
or,
```
DEFINE IPX GLOBAL SAP_TYPE 4 ADD
```
4 = File Service. This filter would block all File Service advertisements that come from the Integration Router's LAN port.

```
DEFINE IPX GLOBAL SAP_TYPE 4 PORT ETHERNET REMOVE
```
or,
```
DEFINE IPX GLOBAL SAP_TYPE 4 REMOVE
```
Removes the filter added above.

```
DEFINE IPX GLOBAL SAP_TYPE 107 PORT WAN ADD
```
107 = NetWare 386 file servers. This filter would block NetWare 386 file server advertisements coming from the WAN (from the remote sites).

```
DEFINE IPX GLOBAL SAP_TYPE 107 PORT WAN REMOVE
```
Removes the filter added above. In this case, DEFINE IPX GLOBAL SAP_TYPE 107 REMOVE would not work – the port must be specified.

```
DEFINE IPX GLOBAL SAP_TYPE 400x ADD
```
Blocks SAP types in the range 4000 through 400f.

```
DEFINE IPX GLOBAL SAP_TYPE 400x REMOVE
```
Removes the filter added above.

```
DEFINE IPX GLOBAL SAP_TYPE NONE
```
Deletes all Global SAP_Type filters.

Routing

Enables or disables IPX packet routing. Before IPX packet routing can be enabled, network numbers must be assigned for each LAN port and for the WAN interface. IPX routing is DEFINED only – the Integration Router must be reset to enable or disable IPX routing.

Command: `DEFINE IPX ROUTING ENABLED/DISABLED`

Privilege: Privileged Command

Default: Disabled

Example: `DEFINE IPX ROUTING ENABLED`

WAN Network Number

Assigns an IPX network number to the WAN interface. You need to define only one IPX network number, no matter how many physical links the WAN interface consists of. All devices on the same WAN and in the same cluster must be configured with the same IPX network number for their WAN interface. Devices in different clusters must have different IPX network numbers configured for their WAN interfaces, as must devices on different WANs. IPX network numbers are 32 bits long and are expressed as a hexadecimal value within the Integration Router. The network number can be entered as a decimal number. The WAN network number is DEFINED only. The Integration Router must be reset for the number to take effect.

When entering network numbers in hexadecimal, you must add 0x to the number before entering it. Example: b000 should be entered 0xb000. If the 0x is omitted, the following message will be displayed:

```
%Error: Bad network number or already assigned to other port
```

Command: `DEFINE IPX WAN NETWORK number`

where *number* = a hexadecimal value between 1 and FFFFFFFE
or, a decimal value between 1 and 4294967294

Privilege: Privileged Command

Default: None

Examples:
```
DEFINE IPX WAN NETWORK 2
DEF IPX WAN NET 0XB000
```

WAN Optimize

The operation of this command is dependent on the configuration of the Integration Router as follows:

IPX Routing = Enabled

WAN Optimize = Enabled: The Integration Router will send only changes to the IPX Routing Table and SAP Table across the WAN to the other routers, in accordance with RFC 1362.

WAN Optimize = Disabled: The Integration Router will periodically send the entire IPX Routing (RIP) Table and the SAP Table across the WAN to the other routers.

IPX Routing = Disabled, SAP Spoofing = Enabled

WAN Optimize = Enabled: The Integration Router will block periodic SAP/RIP broadcasts from being forwarded across the WAN. Only SAP Table changes will be sent across the WAN. Each Integration Router on the WAN will then send out periodic broadcasts on its attached LAN, which contains all the information that would have repetitively been sent across the WAN by the servers.

WAN Optimize = Disabled: The Integration Router will forward periodic SAP/RIP broadcasts across the WAN as a normal bridge would.

WAN Optimize must be set to the same setting at all Integration Routers in the WAN. WAN Optimize is DEFINED only. The Integration Router must be reset to enable or disable WAN Optimize.

Note: You must set WAN bandwidth optimization to *disabled* for all Integration Routers, when a single WAN has MICOM equipment with earlier LAN module software releases (such as the RLB).

Command: `DEFINE IPX WAN OPTIMIZE ENABLED/DISABLED`

Privilege: Privileged Command

Default: Enabled

Example: `DEFINE IPX WAN OPTIMIZE ENABLE`

Show, Monitor, and List

For a description of the SHOW, MONITOR, and LIST commands, please see *Show, Monitor, List Bridge Commands*, page 7-15.

Counters

Displays various IPX counters, such as packets forwarded, RIP packets sent, and RIP packets received. Use the `ZERO COUNTERS IPX` command to reset the IPX counters.

Command: `SHOW/MONITOR IPX COUNTERS`

Privilege: `MONITOR IPX COUNTERS` is a privileged command.

```
Local_2> show ipx counters
IPX   Router Statistics          Ethernet               Wan
packets_to_route                      0                  0
hop_counts_too_large                  0                  0
path_not_found_packets                0                  0
route_entries_aged_out                4                  0
periodic_router_broadcasts sent       0                  0
periodic_router_broadcasts rcvd    2945                  0
update_router_broadcasts              0                 32
SAP_entries_aged_out                  8                  0
SAP_periodic_broadcasts sent          0                  2
SAP_periodic_broadcasts rcvd       6488                  0
SAP_update_broadcasts                 0                 40
SAP_general_queries sent              0                  0
SAP_nearest_queries rcvd             97                  0
SAP_nearest_responses sent            0                  0
packets_sent                          0                 74
packets_received                  10430                  0
packets_forwarded                     0                  0
```

IPX

SHOW IPX displays the values currently in use for the IPX routing parameters. LIST IPX displays the IPX routing parameter values stored in nonvolatile memory.

Command: SHOW/MONITOR/LIST IPX

```
Local> show ipx

Current IPX Router Configuration
Routing             disabled
Wan optimization    enabled
Ethernet :          UP

Mac address         0040c5002923
Network address     0x00000001
Frame Type          RAW_8023

Wan      :          UP

Mac address         0040c5002923
Network address     0xc5002923

Filtering                         enabled
(Exclusive) SAP Filters         0004 : Eth
Network Filters                   None.

Local>

Local> list ipx
NVR Version 1.1

Routing:            enabled
Wan optimization    disabled

Ethernet :

Mac address         0040c5002923
Network address     00000001
Frame Type          RAW_8023

Wan      :

Mac address         0040c5002923
Network address     c5002923

Filtering:                        enabled
(Exclusive) SAP type Filters    0004 : Eth
Network Filters                   None.
```

Routes

Displays the IPX (RIP) routing table. All entries are dynamically learned. You cannot make changes to the parameters displayed in this table.

SHOW IPX ROUTES provides a paged display if there are more than 16 entries in the table. The screen display will stop after each page. Type in any key to display the next page. MONITOR IPX ROUTES does not provide a paged display. Each time the table is displayed, it is scrolled on the screen without pause.

Command: SHOW/MONITOR IPX ROUTES

Privilege: MONITOR IPX ROUTES is a privileged command.

```
Local> show ipx routes

 network   hops  transport_time         next_hop     port     link   timer

c500304f    3          20           0040c500304f     0001     000a    127
07788cba    3          20           00aa003d9593     0001     0004    164
c500080e    5          39           0040c500080e     0001     0004    164
c500350e    2           2           0040c500350e     0001     0007    122
```

SAPS

Displays the IPX SAP table. All entries are dynamically learned. You cannot make changes to the parameters displayed in this table.

SHOW IPX SAPS provides a paged display if there are more than 16 entries in the table. The screen display will stop after each page. Type in any key to display the next page. MONITOR IPX SAPS does not provide a paged display. Each time the table is displayed, it is scrolled on the screen without pause.

Command: SHOW/MONITOR IPX SAPS

Privilege: MONITOR IPX SAPS is a privileged command.

```
Local> show ipx saps

name                              type hops  network  socket    port timer

RTS_5B-c_20B                      0047 0003  c500304f  8060     0001 175
RTS_0040C5000147                  0047 0003  c5000147  8060     0001 150
CERT                              0004 0003  2dae7594  0451     0001 148
VOICE                             0004 0003  10203040  0451     0001 148
TEST                              0107 0004  00ff6550  8104     0001 148
```

Server Commands

Set and Define

For a description of the SET and DEFINE commands, please see *Bridge Commands*, page 7-5.

Announcements

Enables or disables sending of LAT multicast announcements of available services. If no local services are offered, no multicasts are sent in either the enabled or disabled state.

Command: `SET/DEFINE SERVER ANNOUNCEMENTS ENABLED/DISABLED`

Privilege: Privileged Command

Default: Enabled

Bootp

Enables or disables operating software download using Bootp (Booting protocol). You should disable Bootp if the server you intend to use for download via the Integration Router LAN port does not support Bootp, or you do not intend to use Bootp for downloading. Bootp is DEFINED only, as this parameter's setting is checked only after a reset.

Command: `DEFINE SERVER BOOTP ENABLED/DISABLED`

Privilege: Privileged Command

Default: Enabled

Example: `DEFINE SERVER BOOTP DISABLED`

Circuit Timer

Specifies the delay between messages from the Integration Router to other LAT devices. Do not change this parameter while active LAT sessions are in progress.

Command: `SET/DEFINE SERVER CIRCUIT TIMER timer value`

where *timer value* equals 30 to 200 milliseconds.

Privilege: Privileged Command

Default: 80 milliseconds

Domain

Specifies a default domain name for use with TCP/IP connections. NONE clears a previously defined domain name. The domain name can be 64 characters long.

Command: `SET/DEFINE SERVER DOMAIN name/NONE`

Privilege: Privileged Command

Example: `DEFINE SERVER DOMAIN PUBS`

Ethernet

Selects which port (AUI or UTP – 8-pin modular jack) the Integration Router is to use for communications over the LAN. For this command to work, software active port discovery must be set on the LAN module (a jumper must be installed in location E4). Ethernet port is DEFINED only – the Integration Router must be reset to change the port selected.

Command: `DEFINE SERVER ETHERNET port`

Privilege: Privileged Command

Default: UTP

Examples:
```
DEFINE SERVER ETHERNET AUI
DEFINE SERVER ETHERNET UTP
```

Identification

Specifies the identification string broadcast to the LAN along with LAT service messages. If spaces or lowercase characters are desired, the string must be enclosed in quotation marks.

Command: `SET/DEFINE SERVER IDENTIFICATION ID_STRING` or `"id string"`

where *id string* equals a 1 - 40 character string

Privilege: Privileged Command

Example: `SET SERVER IDENTIFICATION "Headquarters Router"`

Incoming

Determines whether incoming LAT or telnet connections are permitted, and allows password configuration for incoming connections. By default, no password is required. The state of incoming connection parameters may be viewed with the SHOW SERVER command. Passwords are configured using the SET/DEFINE LOGIN PASSWORD command.

Command: `SET/DEFINE SERVER INCOMING option`

Privilege: Privileged Command

Default: LAT and telnet connections permitted, no password required.

Options: Both
LAT
None
Nopassword
Password
Telnet

Examples:

`DEFINE SERVER INCOMING BOTH`
(allows both LAT and telnet connections to the Integration Router)

`SET SERVER INCOMING LAT`
(allows LAT connection only)

`DEFINE SERVER INCOMING NONE`
(disables LAN and telnet connections to the Integration Router)

`SET SERVER INCOMING NOPASSWORD`
(no password is required for LAT and telnet connections)

`SET SERVER INCOMING PASSWORD`
(requires a password for LAT and telnet connections)

`DEFINE SERVER INCOMING TELNET`
(allows telnet connections to the Integration Router)

IPaddress

Specifies the main IP address of the Integration Router. When the Integration Router is bridging IP packets, `IPaddress` is the address used for SNMP and by devices to establish telnet sessions with the Integration Router. When the Integration Router is routing IP packets, `IPaddress` is the IP address of the Integration Router's LAN port. `IPaddress` is DEFINED only – you must reset the Integration Router to change the IP address.

Command: `DEFINE SERVER IPADDRESS ip_address`

where *ip_address* is set in standard numerical format (xxx.xxx.xxx.xxx)

Privilege: Privileged Command

Example: `DEFINE SERVER IPADDRESS 193.53.119.240`

Loadhost

Specifies the IP address of the TFTP (Trivial File Transfer Protocol) server from which the Integration Router is to download its operating software. Loadhost is DEFINED only, as this parameter's setting is checked only after a reset.

Command: `DEFINE SERVER LOADHOST ip_address`

where *ip_address* is the IP address of the TFTP server, set in standard numerical format (nnn.nnn.nnn.nnn)

Privilege: Privileged Command

Example: `DEFINE SERVER LOADHOST 199.30.18.21`

Lock

Determines whether local users are able to lock their ports.

Command: `SET/DEFINE SERVER LOCK ENABLED/DISABLED`

Privilege: Privileged Command

Default: Enabled

Login Password

Specifies the password that allows incoming connections from LAT and telnet. This is the password an operator must enter to the Password prompt when establishing a session with the Integration Router via LAT or telnet. If you do not enter a password on the command line, you will be prompted for one after you enter the command. The password can be a maximum of 6 alphanumeric characters.

Command: `SET/DEFINE SERVER LOGIN PASSWORD password`

Privilege: Privileged Command

Maintenance Password

Specifies the password allowing remote console (Network Control Program, or NCP) connections to the Integration Router. Unlike other passwords, the maintenance password is a string of up to sixteen hexadecimal digits (0-9, A-F, a-f) which defaults to all zeros (off). Zero is also NCP's default.

Command: `SET/DEFINE SERVER MAINTENANCE PASSWORD password`

where *password* equals 1-16 hexadecimal digits.

Privilege: Privileged Command

Default: 0 (zero)

Multicast Timer

Specifies the time lapse between transmissions of service announcements for LAT connections. Timer units are in seconds, ranging between 10 and 180.

Command: `SET/DEFINE SERVER MULTICAST TIMER time`

where *time* equals 10 - 180 seconds

Privilege: Privileged Command

Default: 30 seconds

Name

Assigns a name to the Integration Router. For LAT service, the name must appear in quotes if lowercase characters are used. Once defined, the name may be used to log into the Integration Router from the LAT network.

Command: `SET/DEFINE SERVER NAME servername`

where *servername* equals 1-16 alphanumeric characters

Privilege: Privileged Command

Examples:
```
DEFINE SERVER NAME HUMPHREY
SET SERVER NAME "Accounting1"
```

Nameserver

Sets or defines the IP address for a TCP/IP nameserver. The domain name-server is a remote TCP/IP host that attempts to resolve text-string telnet host names into numeric IP addresses if the local host cannot.

Command: `SET/DEFINE SERVER NAMESERVER ip_address`

where *ip_address* equals the standard numeric IP address of the nameserver

Privilege: Privileged Command

Example: `SET SERVER NAMESERVER 193.53.134.204`

Number

Sets or defines the server's node number. Each server on the LAN must have a unique number. Do not set this value while LAT sessions are active.

Command: `SET/DEFINE SERVER NUMBER servernumber`

where *servernumber* equals a value from 0 to 32767

Privilege: Privileged Command

Default: 0 (zero)

Password Limit

Sets the number of attempts a user has to enter a correct privileged password during the execution of the SET PRIVILEGED command. Once the number has been exceeded, the port is logged out of the system. The number of retries allowed ranges from 0 to 100.

Command: `SET/DEFINE SERVER PASSWORD LIMIT number` or `none`

where *number* equals between 0 - 100, and *none* allows unlimited attempts

Privilege: Privileged Command

Default: 3

Privileged Password

Sets or defines the password required for becoming a privileged Integration Router user (with the SET PRIVILEGED command). If the user does not enter a password on the command line, one will be prompted for.

Command: `SET/DEFINE SERVER PRIVILEGED PASSWORD password`

where *password* equals a 1-6 character alphanumeric string

Privilege: Privileged Command

Default: SYSTEM

Prompt

Specifies a prompt to use instead of the Local> prompt. A string up to 16 characters long can be configured and must be enclosed in quotes.

Command: `SET/DEFINE SERVER PROMPT "prompt [option]"`

Privilege: Privileged Command

Option: The following options can be included in the prompt string:

%p	substitutes the current port's name
%n	substitutes the current port's number
%s	substitutes the current server name
%S	substitutes the current session name
%P	substitutes a > if user is currently privileged
%%	substitutes a %

Default: Local>

Examples:
```
SET SERVER PROMPT "Acct-" Prompt = Acct-
SET SERVER PROMPT "Local %n>%P" Prompt = Local 3>>
```

Retransmit Limit

Specifies the number of attempts a LAT packet will be retransmitted if not acknowledged within the pre-set time. On heavily used LANs, a higher limit should be used.

Command: `SET/DEFINE SERVER RETRANSMIT LIMIT limit` or `none`

where *limit* equals a number between 4 and 100, and *none* sets no limit on retransmission.

Privilege: Privileged Command

Default: 8

Software Path

Specifies the name of the file on the TFTP server to download (when downloading the Integration Router's operating software). A path is optional and would be used if the file is not in the TFTP server's default directory, or there is no default directory. Most TFTP servers have a default directory (for example, /tftpboot). Software path is DEFINED only, as this parameter's setting is checked only after a reset.

Note: The filename extension should not be entered. The extension should alwlays be .SYS.

Command: `DEFINE SERVER SOFTWARE [/path/]filename`

Privilege: Privileged Command

Examples:
```
DEFINE SERVER SOFTWARE /tftpboot/MICOMLD
DEFINE SERVER SOFTWARE MICOMLD
DEF SER SOFTWARE MICOMLD
```

Subnet Mask

Sets an IP subnet mask for the main IP address or the LAN port of the Integration Router (`SET/DEFINE SERVER IPADDRESS`). A mask will be set by default when the IP address is set, and will be the correct one for most environments. This command overrides the default value. The mask is applied to target IP addresses to determine whether the destination address is on the local network segment or not. If not, the designated gateway host will be accessed to provide the connection.

Command: `SET/DEFINE SERVER SUBNET MASK mask`

where *mask* is the subnet mask (for example, 255.255.255.0)

Privilege: Privileged Command

Default: Based on the IP address that has been set/defined for the LAN port of the Integration Router.

Show, Monitor, and List

The SHOW/MONITOR/LIST commands display various fields describing Integration Router status.

SHOW commands are used to display current settings and statistics.

MONITOR commands are the same as SHOW commands except information is continuously updated every three seconds. The display can be stopped by pressing any key. MONITOR is a privileged command.

LIST commands are used to display the characteristics stored in nonvolatile memory, which may or may not be the same as those currently set. For example, if you use the SET command to temporarily change certain parameters, the changes will not appear with the LIST command. Please note that the LIST command is not used with every option described below.

Characteristics

Displays the configured characteristics for the server.

Command: SHOW/MONITOR/LIST SERVER

Privilege: Privileged Command

```
Local_2> show server

   Boot Rom Ver 1.0 144-0153-0A
   RLB Ver 6.0 908-2238-0A                Uptime:                    2:09:05
   Hardware Address: 00-40-c5-10-0c-3f    Daytime:                  14:38:11
   RTS Name: RTS_0040C5100C3F             CCM Nodename:               MICOM2
   Ident String: Ethernet Interface

   Circuit Timer (msec):           80     Password Limit:                3
   Multicast Timer (sec):          30     Queue Limit:                 N/A
   Inactive Timer (min):           30     Retrans Limit:                 8
   Keepalive Timer (sec):          20     Session Limit:               N/A
   Node Number:                     0     Max Ports:                    64

   LAN IP Address:      199.30.19.214     Subnet Mask:       255.255.255.0
   WAN IP Address:        (undefined)     Subnet Mask:         (undefined)
   Nameserver:            (undefined)     Domain Name:         (undefined)
   TFTP Loadhost:        199.30.19.46     BOOTP:                   enabled

   Software File:      199.30.19.46:/tftpboot/MICOMLD.SYS


   Characteristics:  Announce  Broadcast  Lock  AUI
   Incoming Logins:  LAT  Telnet   (No Passwords Required)
```

Counters

Displays the following network and access/connection counters.

Command: SHOW/MONITOR SERVER COUNTERS

Privilege: Privileged Command

```
Local> show server counters
   Boot Rom Ver 1.0 144-0153-0A
   RLB Ver 6.0 908-2238-0A                Uptime:          13 Days  20:23
   Hardware Address: 00-40-c5-10-0c-3f    Daytime:               8:52:07
   RTS Name: RTS_0040C5100C3F             CCM Nodename:            TPNET
   Ident String: Ethernet Interface

                        Received      Sent   Seconds since zeroed: 1196605
   Bytes:                      0  33581056   Frames Deferred             0
   Frames:                     0    524704   Send Failure Reasons:    0000
   Multicast Bytes:      5670195   5667938   Recv Failure Reasons:    0000
   Multicast Frames:       41898     41883   Data Overrun:               0
   Network Failures:           0         0   Unknown Protocols:          0
   Frames Sent 1 Coll:                   0   NIC Buffer Unavailable:     0
   Frames Sent 2+ Coll:                  0   Sys Buffer Unavailable:     0

LAT  Messages:                 0         0   Solicit Accepted:           0
     Retransmissions:          0         0   Solicit Rejected:           0
     Illegal Slot:             0         0   Illegal Messages Recv:      0

TCP  Messages:                 0         0   Connect Failure Reasons: 0000
     Invalid Packets:          0         0   Invalid Packet Reasons:  0000
```

Where:

Bytes – total bytes received and sent.

Frames – total number of all frames received and sent to this Integration Router.

Multicast Bytes – total number of multicast bytes received.

Multicast Frames – total number of multicast frames received.

Network Failures – number of bad LAN packets.

Frames Sent 1 Coll – number of frames seeing one collision when transmitting.

Frames Sent 2+ Coll – number of frames seeing more than one collision when transmitting.

Seconds since zeroed – amount of time since counters were last zeroed

Send Failure Reasons – see error code description below

Recv Failure Reasons – see error code description below

Data Overrun – Network Interface Circuit (NIC) memory access error

Unknown Protocols – number of packets received that the Integration Router could not interpret

NIC Buffer Unavailable – number of dropped packets due to memory constraints

Sys Buffer Unavailable – number of dropped packets due to memory constraints

LAT Messages – number of LAT messages transmitted

Retransmissions – number of LAT retransmissions

Illegal Slot – illegal LAT slot number

Solicit Accepted – number of LAT solicits accepted

Solicit Rejected – number of LAT solicits rejected

Illegal Messages Recv – number of illegal messages received

TCP Messages – number of TCP/IP packets received and sent by the Integration Router

Invalid Packets – number of invalid TCP/IP packets received

Connect Failure Reason – see error code description below

Invalid Packet Reasons – see error code description below

Error Codes

Part of the display includes error messages of selected events expressed in hexadecimal form. Each error message has a different number of significant digits formatted as follows:

```
0 0 h h (0 = unused, h = hexadecimal digit)
```

The following tables describe the error codes for each event.

Send Failure Reasons:	
Bits 0–1:	Unused, should be 0.
Bit 2:	At least 1 collision has occurred while transmitting.
Bit 3:	Transmit aborted due to excessive (more than 16) LAN collisions.
Bit 4:	Carrier Sense was lost during transmission.
Bit 5:	FIFO underrun: Ethernet controller could not access transmit data in time to send it out.
Bit 6:	The Integration Router did not receive CD heartbeat after transmission.
Bit 7:	Out of Window Collision detected.
Bit 8:	Network off line.
Bits 9–15:	Unused, should be 0.

Recv Failure Reasons:	
Bit 0:	Unused, should be 0.
Bit 1:	Packet received with CRC error.
Bit 2:	Received packet did not end on byte boundary.
Bit 3:	FIFO overrun: could not write received data before new data arrived.
Bit 4:	Receive packet could not be accommodated due to not enough receive buffers.
Bit 5:	Received a packet larger than the maximum Ethernet size (1536 bytes).
Bits 6–15:	Unused, should be 0.

Connect Failure Reasons:	
Bits 0–1:	Internal failures, should be 0.
Bit 2:	No nameserver defined for a text hostname.
Bit 3:	Attempted nameservice failed.
Bit 4:	No gateway was configured for a non-local connection.
Bit 5:	Attempted ARP failed.
Bit 6:	Remote Host did not answer.
Bit 7:	Host rejected the connection.
Bits 8–15:	Unused, should be 0.

Invalid Packet Reasons:	
Bit 0:	Data received outside window.
Bit 1:	Well known port is unavailable.
Bit 2:	Packet received for an unknown local user.
Bit 3:	Packet received with an invalid data checksum.
Bit 4:	Packet received with an invalid data header.
Bit 5:	Connection was terminated abnormally.
Bits 6–15:	Unused, should be 0.

Status

Displays the following server status.

Command: SHOW/MONITOR SERVER STATUS

Privilege: Privileged Command

```
Local> show server status
   Boot Rom Ver 1.0 144-0153-0A
   RLB Ver 6.0 908-2238-0A                Uptime:           13 Days  21:07
   Hardware Address: 00-40-c5-10-0c-3f    Daytime:                 8:55:04
   RTS Name: RTS_0040C5100C3F             CCM Nodename:              TPNET
   Ident String: Ethernet Interface

                       Cur  High  Max                        Cur  High  Max
   Active Ports:         2     2   64      Active Users:      1     1   64
   Active Circuits:      0     0  256      Queue Entries:     0     0   20
   Available Services:   1     1  ---      Local Services:    0     0   64

   Time to Shutdown:              N/A

   Memory Usage (%):     49       100      Allocated Pkts:          357203
   Free Bytes:       231448    414136      Freed Pkts:              356918
   Memory Fragments:                7      Largest Packet:           81444
   NVRAM Memory:      15211     15360      Allocation Failures           0
   NVRAM Backup:                   no      Com Line Memory:          27948
```

Where:

Active Ports – current login ports

Active Circuits – all open connections to and from another host.

Available Services – total number of network services available.

Active Users – the number of current users.

Queue Entries – not applicable to the Integration Router.

Local Services – not applicable to the Integration Router.

Time to Shutdown – not applicable to the Integration Router.

Memory Usage (%) – current percentage of all free memory in use.

Free Bytes – current and maximum available free memory in system pool.

Memory Fragments – number of fragments that make up the system memory pool.

NVRAM Memory – available space in nonvolatile memory for saved configuration information.

Allocated/Freed Packets – number of packets removed from and returned to the system pool.

Largest Packet – the size of the largest single packet in the system pool.

Allocation Failures – number of times a packet could not be allocated due to lack of memory.

Com Line Memory – number of bytes in the command line memory pool.

General Commands

The following commands refer to general Integration Router operation.

CLS

Clears the screen for ANSI terminal devices.

Command: `CLS`

Connect WAN

Requests a connection to the command port of the CCM.

Command: `CONNECT WAN $CMD`

Privilege: Privileged Command

Finger

This command is an implementation of the UNIX finger command which shows local and remote users. The finger command, by itself, will show processes running on the Integration Router, including network user processes. If a user name is specified, information about the user is shown. If the finger command is given with a parameter such as user@host, information regarding that user on that TCP/IP host will be shown. The user name can be omitted, in which case all the users on the host are displayed.

Command: `FINGER user` or `@host` or `user@host`

Note: An error is displayed if the host cannot be accessed.

Examples:
`FINGER` (displays processes running on the Integration Router)
`FINGER` *`user1`* (displays user1's processes running on the Integration Router)
`FINGER` *`@host3`* (displays users on host3)
`FINGER` *`user1@host3`* (shows information about user1 on host3)

Help

Displays an on-line help menu with descriptions of each command and subcommand. Executing help displays the top level of commands and prompts for a topic. By entering a command, a list of subcommands is shown where applicable.

Command: `HELP`

Initialize Server

Causes an orderly shutdown and reboot of the server (that is, the Integration Router), or cancels a pending INITIALIZE command. When reset, the Integration Router loses all changes made with the SET commands (unless corresponding DEFINE or SAVE commands were also made). The DELAY option allows you to schedule the INITIALIZE after a specified number of minutes (SHOW SERVER STATUS will show the time pending until a scheduled reboot). The CANCEL parameter cancels any pending INITIALIZE command. Option DELAY sets the number of minutes to delay the reboot.

Command: `INITIALIZE SERVER option delay_time`

where *option* equals either option listed below, and *delay_time* is 0 - 120 minutes.

Privilege: Privileged Command

Options: Delay
Cancel

Example: `INITIALIZE SERVER DELAY 12` (shutdown will occur in 12 minutes)
`INITIALIZE SERVER CANCEL` (cancels a pending initialize command)

Lo

This command is an alias for LOGOUT, described below.

Lock

Locks any terminal user session, preventing access by unauthorized personnel without disconnecting sessions. The user is queried for a password (6 characters maximum, alphanumeric characters only) and asked to verify it. The password and verification are not displayed. Access is then locked until the correct password is used to unlock it. If a user forgets the password, the privileged user must either use the LOGOUT or the UNLOCK PORT command.

Command: `LOCK`

Privilege: Secure users may not lock ports

Logout

Logs the specified user out of the Integration Router. LOGOUT by itself will terminate your own session with the Integration Router. The privileged user can logout other users by specifying either the PORT of the Integration Router that the user's session is connected to, or the CHANNEL of the unit the user's terminal is attached to.

Command: `LOGOUT CHANNEL/PORT number`

Example: `LOGOUT CHANNEL B2` (logs out user whose terminal is connected to async port B2 on the unit)

Man

This command is an alias for HELP, described above.

Ping

PING sends a request (using TCP/IP) for an echo packet to another TCP/IP network host, providing an easy way to test network connections between TCP/IP hosts. In general, any host supporting TCP/IP will respond if able, regardless of login restrictions, job load, or operating system. If there is no reply from the host, this may indicate a network or TCP/IP configuration problem. Note that either a text host name or IP address can be used.

Command: `PING hostname` or `ip_address`

Privilege: Privileged Command

Example:
```
PING host1
PING 192.53.139.205
```

Purge Sysdump

Clears the information stored for the system dump. You should enter this command after capturing or viewing the system dump to reset the Integration Router for the next network failure.

Command: `PURGE SYSDUMP`

Privilege: Privileged Command

Save

Saves the current configuration that was entered using SET commands into nonvolatile memory.

> ⚠ **CAUTION**
>
> All previously defined values in nonvolatile memory are set to the current values when the save command is executed.

Command: `SAVE BRIDGE` or `SERVER` or `IP` or `IPX`

Privilege: Privileged Command

Set Ports

Allows you to configure the session ports. If SET PORT is followed by a port number or name, that will be the port that is configured. If no number or name follows SET PORT, the current port that you are using will be modified.

Command: `SET PORTS number OPTIONS`

Options: Command Completion Enabled – enables completion of partially typed commands when a space or tab character is typed. Example: "sh br st" is completed as "show bridge status."

Command Completion Disabled – disables completion of partially typed commands. Each command with all required parameters must be entered in its entirety.

Termtype – specifies a terminal type string to provide for telnet and rlogin sessions.

Type – specifies the type of device attached to the port. The device types are:

ANSI – VT100 compatible (supports Escape sequences, screen clears, etc.).

Hardcopy – suitable for a text printer. No cursor motion commands, scrolling, etc. The only codes sent to the device are ASCII characters.

Softcopy – for non-VT100 terminals. Provides scrolling, line editing, etc.

Username – specifies a name to be associated with this port. A user name can be 1 to 16 alphanumeric characters. User names must be enclosed in quotes if lower case characters are to be used.

Example: `SET PORTS 1 TYPE ANSI` (configures port number 1 on the Integration Router to ANSI terminal type – VT100 compatible)

Set Privileged

Specifies the current port as a privileged port, enabling privileged operations. Only one Integration Router port may be privileged (see OVERRIDE below).

Command: `SET NOPRIVILEGED` or `PRIVILEGED` or `PRIVILEGED OVERRIDE`

Options: Noprivileged – Resets a privileged port to non-privileged status.

Privileged – Enables a port to perform privileged operations.

Privileged Override – Forces the current port to become privileged if another port is set to privileged.

Show/Monitor/List

Show commands are used to display the current settings and statistics. Monitor commands are the same as show commands except information is continuously updated every three seconds. The display can be stopped by pressing any key. Monitor is a privileged command. List commands are used to display the DEFINED (stored in nonvolatile memory) characteristics, which may or may not be the same as those currently set.

Ports

Command: `SHOW/MONITOR/LIST PORTS port option`

where *option* is one of the options listed below

Privilege: Privileged Command

Options: Characteristics – Displays information gathered from the operation database.

Counters – Displays network and access connection counters.

Port – You can enter 0 (for the NetConsole), a physical port number, or ALL (to list all ports). If you do not specify a port, the display will be for the port you are using.

Status – Displays full information for the specified node, including network address, protocol version, and all services offered by the node.

Summary – Displays a one-line summary of the type of access, status, and services offered by the specified port.

Sample displays are shown below.

`Local> show ports characteristics` (same as SHOW PORTS)

```
Port 1 : Username: Dave                Physical Port 1 (Local Mode)

   Access:                   Remote    Port Name:                Console
   Forward:                    None    Terminal Type:             Soft()

   Preferred Services:         (Lat)
                             (Telnet)

   Authorized Groups : 0
   (Current)  Groups : 0

   Characteristics:  Autoprompt  Loss Notify  Verify  Privs
                     Remote Conf  Telnet Pad
```

```
 Local> show ports counters

Port 1 : Username: Dave                Physical Port 1 (Local Mode)

   Seconds Since Zeroed:    1201477    Framing Errors:                0
   Local Accesses:                0    Parity Errors:                 0
   Remote Accesses:               0    Overrun Errors:                0
                                       Flow Control Violations:       0

   Bytes Input:                 144    Bytes Output:               4645
   Input Flow On/Off:      0/     0    Output Flow On/Off:      8/     8

Local> show ports status

Port 1 : Username: Dave                Physical Port 1 (Local Mode)

   Access:                   Remote    Current Service:            None
   Status:                  Virtual    Current Node:               None
   Sessions:                      0    Current Port:               None

Local> show ports summary

 Port   Name          Username        Status

-> 1    Console       Dave            Local Mode
```

Sysdump

Displays current system dump information only if a serious network failure occurs. If the network has not recently failed, no sysdump log will have been created. To clear the system dump information, enter the command PURGE SYSDUMP.

Command: `SHOW/MONITOR SYSDUMP`

Privilege: `MONITOR SYSDUMP` is a privileged command.

Users

Displays current information about port users, including access status and services in use.

Command: `SHOW/MONITOR USERS`

Privilege: `MONITOR USERS` is a privileged command.

Su

This is an alias for the SET PRIVILEGED command.

Test

Executes a port or loop network test. A helper node may be specified to forward one or both transmissions (outbound or incoming). Tests are terminated by pressing any key on the device initiating the test.

Command: `TEST option ethernet_address helpnode`
or
`TEST PORT count/width number`

Privilege: Privileged Command

Options: Loop – Requests a test connection to a remote host.
Helpnode – Name of the node that will forward the transmissions.
Port – Tests a port on the server.
Count – Specifies the number of test lines sent.
Width – Specifies the number of characters per line in the test pattern.

Examples: `TEST LOOP 00-A2-ED-48-12-3C`
(performs a loop test between the Integration Router and the specified device)

`TEST PORT count 12 width 30`
(tests the port with 12 lines, 30 characters per line)

Unlock Port

Allows an administrator to unlock a locked terminal session if the session was locked by a user.

Command: `UNLOCK PORT number`

Privilege: Privileged Command

WAN

Requests a connection to the command port of the CCM.

Command: `WAN $CMD`

Who

An alias for SHOW USERS.

Command: `WHO`

Privilege: Privileged Command

Zero Counters

Resets counters on the Integration Router. The ALL command resets all system counters.

Command: `ZERO COUNTERS ALL` or `BRIDGE` or `IP` or `IPX`

Options: All – Zeros all server, port, and network counters.

Bridge – Clears the counters for bridge links.

IP – Clears the IP router counters.

IPX – Clears the IPX router counters.

Specifications A

EasyRouter Technology

Routed Protocols:
IP, per RFC 1009
IPX, per *IPX Router Specification* version 1.10 (Novell part number 107–000029–001) and RFC 1362.

Routing Protocol:
RIP

Management Protocol:
SNMP, monitor (GETs) only

Bridged Protocols:
IP, IPX (including oversize packets in Novell NetWare), LAT, Appletalk, NETBIOS, DECnet.

Broadcast reduction and storm prevention:
In bridged IP networks, the Integration Router responds locally to ARP requests sent by a local device to a remote host. These ARP requests are not forwarded across the WAN. Also, the Integration Router blocks ARP requests to local hosts from appearing on the WAN and restricts the number of outstanding (not responded to) ARP requests to a remote host to prevent broadcast storms.

In bridged IPX networks, the Integration Router responds locally to most SAP/RIP requests sent by local IPX workstations to find particular services or networks. These SAP/RIP requests are not forwarded across the WAN. The Integration Router restricts the number of outstanding (not responded to) SAP/RIP requests for remote services or networks to prevent broadcast storms.

Ethernet Interface

Software selectable for IEEE 802.3 compatible 15-pin AUI connector or 8-pin modular jack for unshielded twisted pair LANs.

Lithium Battery	The LAN module contains a lithium battery that supplies power to the CMOS RAM for an accumulated power-down life of eight years. User life of the battery is ten years (not rechargeable).
Compression	LAN data compressed up to 4:1. Compression of IP, IPX, and LAT headers up to 10:1.
Filters	Automatic filtering on destination address. User-invoked filtering for broadcast, multicast, source address, protocol type, pattern match.
Spanning Tree	IEEE 802.1D compliant. Compatible with all 802.1D compliant bridges.
Management	Locally via Command Facility. Remotely via any unit in the network and via NETMan. From LAN via LAT or telnet connection. SNMP agent with public domain MIB II (monitor - GETs - only).
Performance	Filtering Rate: 8,000 frames per second, 64 byte packets Forwarding Rate: 185 to 490 frames per second. Forwarding rate is dependent on specific model, which FEATUREPAK/FlashPak cartridge is used in the LAN module, and other traffic types.

FlashPak Cartridge Installation and Jumper Selection B

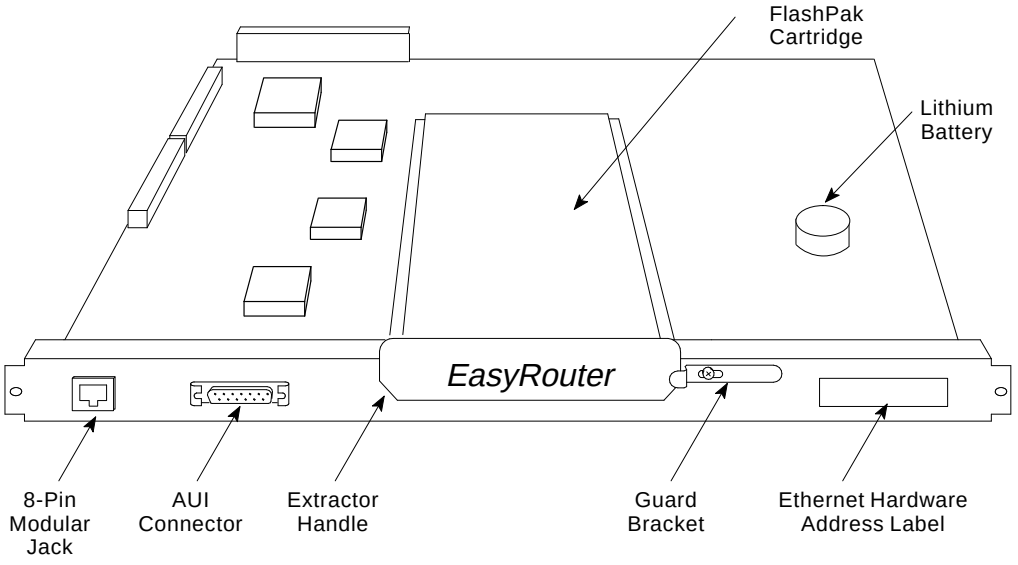
This appendix describes the following procedures for installing the LAN module.

For NetRunner 75E, please see the NetRunner 75E Installation Manual for information about EasyRouter FlashPak cartridge installation. The NetRunner 75E does not require setting any switches or jumpers for the LAN functions.

Page

Module Location Switch Settings B-2
Installing the EasyRouter FlashPak Cartridge B-3
Setting the Jumpers B-5

The LAN module with the EasyRouter FlashPak cartridge installed is shown below.



Safety Information

The Underwriters Laboratories, Inc. (UL), Canadian Standards Association (CSA), Technische Überwachungsverein (TÜV) of Germany, and British Approval Board for Telecommunication (BABT) request the following statements of warning or caution be made in English, German, and French to help you in the safe operation of the unit. These statements also apply to any and all modules installed within the unit.

Access to the interior of this unit shall be made only by a qualified technician.	Der Zugang ins Innere des Gerätes ist nur einem qualifizierten Techniker gestattet.	Ouverture de cet appareil est permise par un technicien autorisé seulement.
Warning	***Warnung***	***Avertissement***
Remove power plug from the power socket before performing any service work on the unit.	Vor öffnen des Gerätes, muss der Netzstecker aus der Steckdose gezogen werden.	Débrancher la prise de courant avant d'entreprendre aucun travail de réparation de l'appareil.
Connection to the network is to be disconnected before the (mains) plug is removed.	Ehe der Netzstecker aus der Steckdose gezogen wird, müssen sämtliche äusserliche Verbindungen vom Gerät getrennt werden.	Avant de débrancher la prise de courant, assurer que toutes les connexions externes ont été déconnecté de l'appareil.

For further precaution, make sure to take steps preventing electrostatic discharge when working inside the unit.

- A wrist strap, properly grounded, should be worn when working inside the unit.
- If a wrist strap is not available, touch any metal part of the unit before handling modules to discharge static electricity.
- Avoid working on carpet.

Installing the LAN Module

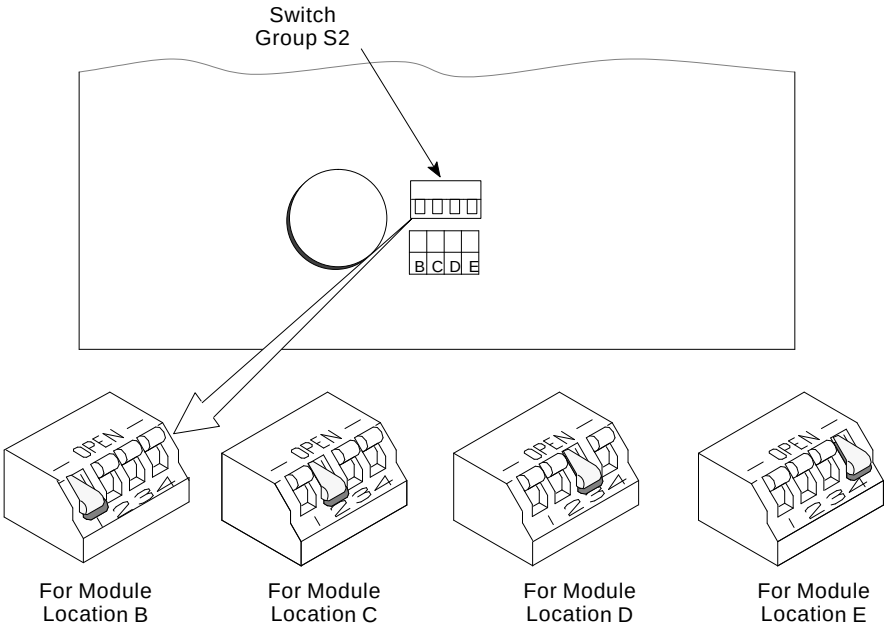
Before handling the LAN module, please make sure to observe the electrostatic precautions described above. Then remove the LAN module and the EasyRouter FlashPak cartridge from the antistatic bags.

Module Location Switch Settings

Each expansion module has a module location switch group informing the software of its location in the unit. The exceptions to this are the CCM, which is always in module location A, and the modem module, which must be the topmost module (no module located above the modem will be operable). The physical location of switch group S2 on the LAN module is shown in the next figure.

Switch group S2 consists of four switches. The silkscreen in front of S2 maps the switches with the module locations. Before setting S2, first determine where the LAN module is to be installed. Set S2 to match the intended module location. To set a switch segment to ON (down, or closed), use a ballpoint pen or similar pointed tool and push the switch segment down.

Note: Make sure that only one switch in switch group S2 is ON (down, or closed) and that the remaining three segments are OFF (up, or open).

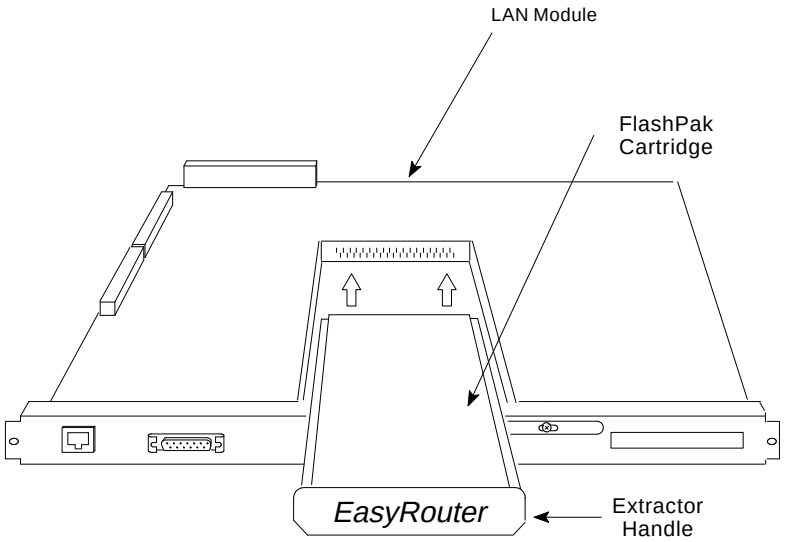


Switch S2 and Module Location Settings

Installing the EasyRouter FlashPak Cartridge

Install the EasyRouter FlashPak cartridge into the LAN module prior to installing the module into the unit:

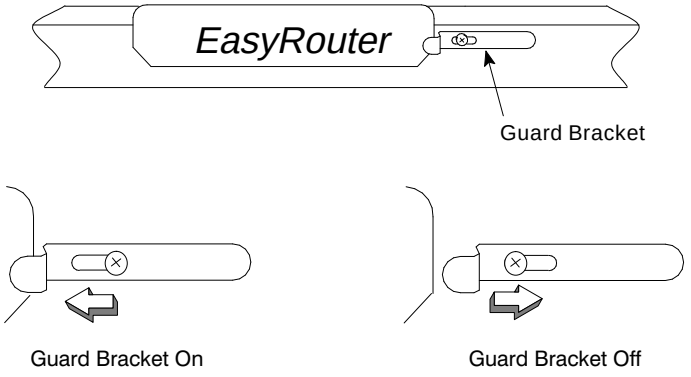
1. Verify the extractor handle is snapped closed flush against the end of the cartridge.
2. Secure the LAN module with one hand and insert the connector end of the FlashPak cartridge into the slot on the module's back panel.
3. Slide the cartridge into the module until the cartridge is fully seated and the extractor handle is flush against the module's back panel. Only a minimum amount of pressure is needed to fully seat the cartridge.



FlashPak Cartridge Installation

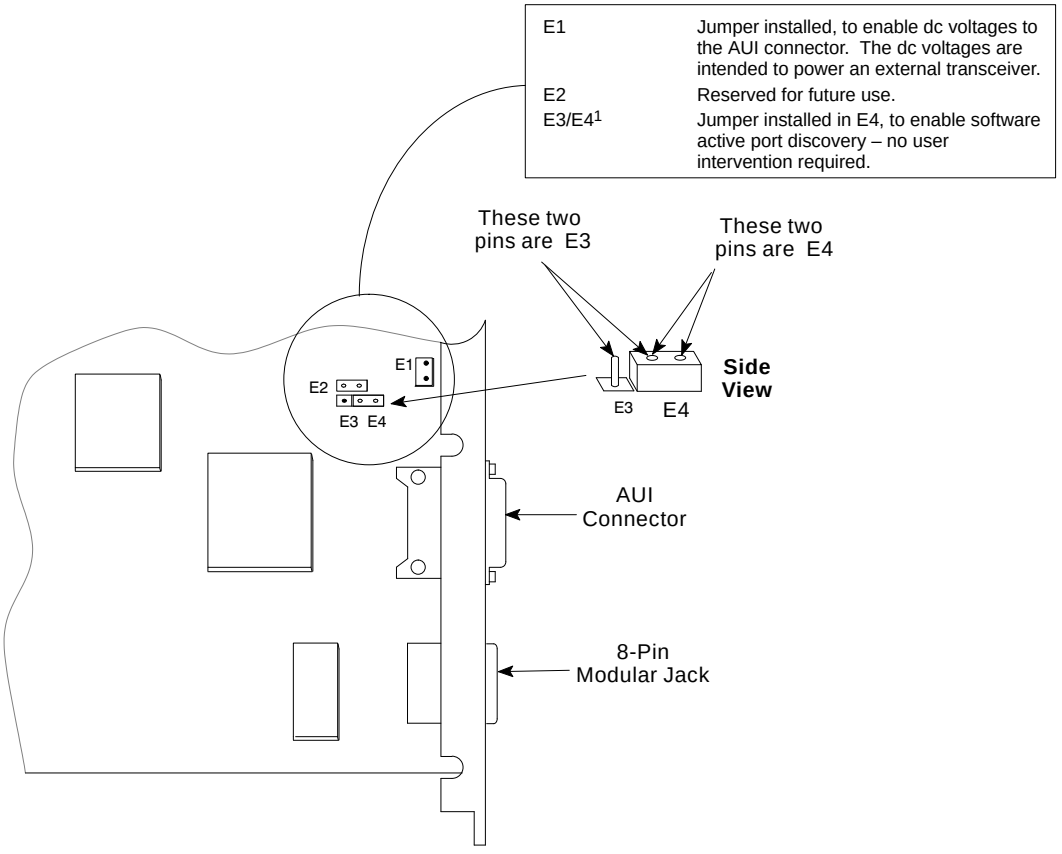
4. Use a number 1 or 2 Phillips screwdriver to loosen the screw holding the guard bracket on the module's back panel (it is not necessary to remove the screw).

5. Slide the guard bracket left until the raised edge is over the cartridge and tighten the screw. The guard bracket is a safety requirement to prevent accidental dislodging of the FlashPak cartridge.



Setting the Jumpers

Set the jumper configuration of the LAN module as follows:


E1 Jumper installed, to enable dc voltages to the AUI connector. The dc voltages are intended to power an external transceiver.
E2 Reserved for future use.
E3/E4[1] Jumper installed in E4, to enable software active port discovery – no user intervention required.
These two pins are E3
These two pins are E4
E1
E2
E3 E4
Side View
E3
E4
AUI Connector
8-Pin Modular Jack

Setting Jumpers

The module is now ready to install in the unit. Refer to the Installation and Cabling Manual for instructions on installing modules in the unit.

[1] If the jumper is in E3, the LAN module will look for a LAN connection only on the 8-pin modular jack. If the jumper is not installed, the LAN module will look for a LAN connection only on the AUI connector. In either case, a LAN connection must exist on the selected port (a transceiver on the AUI connector, or a hub connection on the 8-pin modular jack) when the Integration Router is reset, or the Integration Router will not come up.

SNMP Management Information Base C

This appendix contains lists of the Management Information Base (MIB-II) for SNMP Management of TCP/IP-based Internets groups that the Integration Router supports. *The Integration Router supports only the **GET** functions of SNMP.*

Detailed information about the SNMP objects supported can be found in RFCs 1066, 1157, 1213, and 1286.

The System Group

sysDescr
sysObjectID
sysUpTime
sysContact
sysName
sysLocation
sysServices

The Interfaces Group

ifNumber
ifTable
ifEntry
ifIndex
ifDescr
ifType
ifMtu
ifSpeed
ifPhysAddress
ifAdminStatus
ifOperStatus
ifLastChange
ifInOctets
ifInUcastPkts
ifInNUcastPkts
ifInDiscards
ifInErrors

IfInUnknownProtos
ifOutOctets
ifOutUcastPkts
ifOutNUcastPkts
ifOutDiscards
ifOutErrors
ifOutQLen
ifSpecific

The Address Translation Group

atTable
atEntry
atIfIndex
atPhysAddress
atNetAddress

The IP Group

ipForwarding
ipDefaultTTL
ipInReceives
ipInHdrErrors
ipInAddrErrors
ipForwDatagrams
ipInUnknownProtos
ipInDiscards
ipInDelivers
ipOutRequests
ipOutDiscards
ipOutNoRoutes
ipReasmTimeout
ipReasmReqds
ipReasmOKs
ipReasmFails
ipFragOKs
ipFragFails
ipFragCreates

The IP Address Table

ipAddrTable
ipAddrEntry
ipAdEntAddr

ipAdEntIfIndex
ipAdEntNetMask
ipAdEntBcastAddr
ipAdEntReasmMaxSize
ipRouteTable
ipRouteEntry
ipRouteDest
ipRouteIfIndex
ipRouteMetric1
ipRouteMetric2
ipRouteMetric3
ipRouteMetric4
ipRouteNextHop
ipRouteType
ipRouteProto
ipRouteAge
ipRouteMask
ipRouteMetric5
ipRouteInfo
ipNetToMediaTable
ipNetToMediaEntry
ipNetToMediaIfIndex
ipNetToMediaPhysAddress
ipNetToMediaNetAddress
ipNetToMediaType
ipRoutingDiscards

The ICMP Group

icmpInMsgs
icmpInErrors
icmpInDestUnreachs
icmpInTimeExcds
icmpInParmProbs
icmpInSrcQuenchs
icmpInRedirects
icmpInEchos
icmpInEchoReps
icmpInTimestamps
icmpInTimestampReps
icmpInAddrMasks
icmpInAddrMaskReps
icmpOutMsgs
icmpOutErrors

icmpOutDestUnreachs
icmpOutTimeExcds
icmpOutParmProbs
icmpOutSrcQuenchs
icmpOutRedirects
icmpOutEchos
icmpOutEchoReps
icmpOutTimestamps
icmpOutTimestampReps
icmpOutAddrMasks
icmpOutAddrMaskReps

The TCP Group

tcpRtoAlgorithm
tcpRtoMin
tcpRtoMax
tcpMaxConn
tcpActiveOpens
tcpPassiveOpens
tcpAttemptFails
tcpEstabResets
tcpCurrEstab
tcpInSegs
tcpOutSegs
tcpRetransSegs
tcpConnTable
tcpConnEntry
tcpConnLocalAddress
tcpConnLocalPort
tcpConnRemAddress
tcpConnRemPort
tcpInErrs
tcpOutRsts

The UDP Group

udpInDatagrams
udpNoPorts
udpInErrors
udpOutDatagrams
udpTable
udpEntry
udpLocalAddress
updLocalPort

The SNMP Group

snmpInPkts
snmpOutPkts
snmpInBadVersions
snmpInBadCommunityNames
snmpInBadCommunityUses
snmpInASNParseErrs
snmpInTooBigs
snmpInNoSuchNames
snmpInBadValues
snmpInReadOnlys
snmpInGenErrs
snmpInTotalReqVars
snmpInTotalSetVars
snmpInGetRequests
snmpInGetNexts
snmpInSetRequests
snmpInGetResponses
snmpInTraps
snmpOutTooBigs
snmpOutNoSuchNames
snmpOutBadValues
snmpOutGenErrs
snmpOutGetRequests
snmpOutGetNexts
snmpOutSetRequests
snmpOutGetResponses
snmpOutTraps
snmpEnableAuthenTraps

The Bridge Group

dot1dBaseBridgeAddress
dot1dBaseNumPorts
dot1dBaseType

The Generic Bridge Port Table

dot1dBasePortTable
dot1dBasePortEntry
dot1dBasePort
dot1dBasePortIfIndex
dot1dBasePortCircuit

dot1dBasePortDelayExceededDiscards
dot1dBasePortMtuExceededDiscards
dot1dStpProtocolSpecification
dot1dStpPriority
dot1dStpTimeSinceTopologyChange
dot1dStpTopChanges
dot1dStpDesignatedRoot
dot1dStpRootCost
dot1dStpRootPort
dot1dStpMaxAge
dot1dStpHelloTime
dot1dStpHoldTime
dot1dStpForwardDelay
dot1dStpBridgeMaxAge
dot1dStpBridgeHelloTime
dot1dStpBridgeForwardDelay

The Spanning Tree Port Table

dot1dStpPortTable
dot1dStpPortEntry
dot1dStpPort
dot1dStpPortPriority
dot1dStpPortState
dot1dStpPortEnable
dot1dStpPortPathCost
dot1dStpPortDesignatedRoot
dot1dStpPortDesignatedCost
dot1dStpPortDesignatedBridge
dot1dStpPortDesignatedPort
dot1dStpPortForwardTransitions

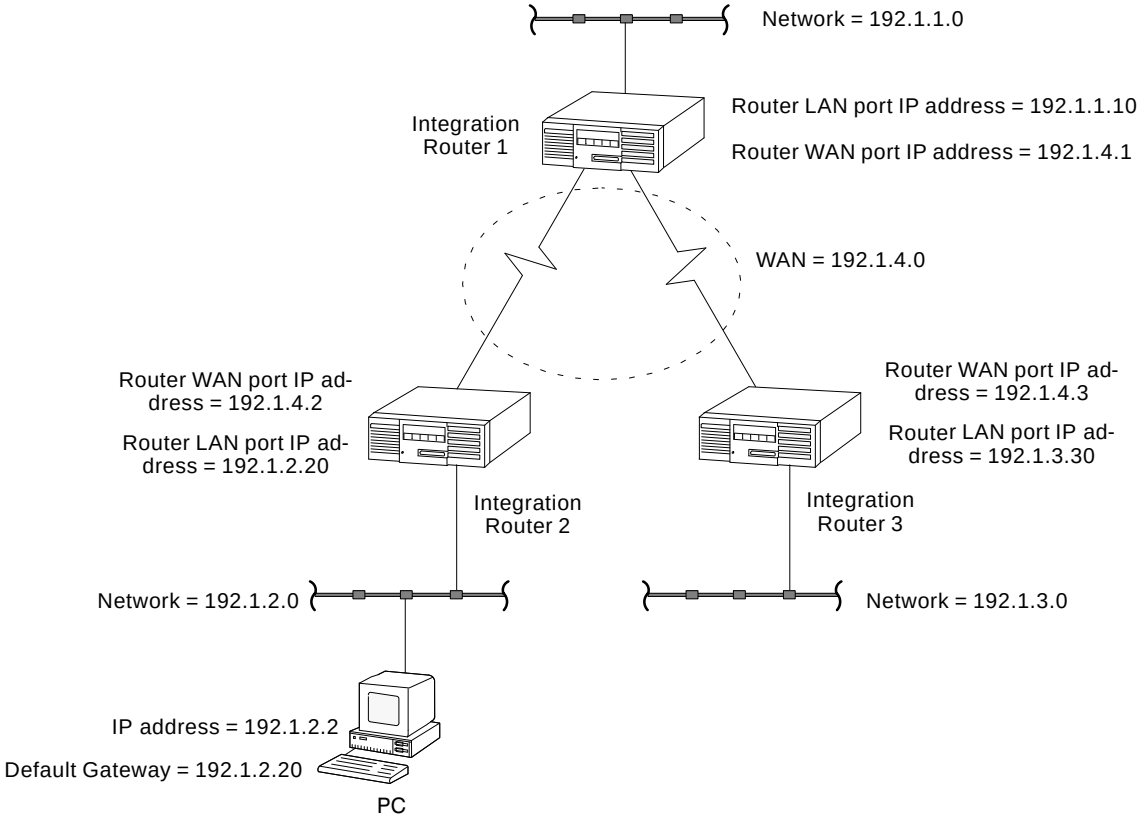
Applications D

Using Telnet To Access the Integration Router's Command Line Interface

When the Integration Routers in a network are bridging IP packets, or in EasyRouter mode, you can telnet into the Integration Routers using the IP addresses defined for their LAN ports. The command for defining the IP addresses is `DEFINE SERVER IPADDRESS ipaddress` (see page 7-39 for details about this command).

When the Integration Routers are routing IP packets (traditional IP routing), the addresses to telnet into the Integration Routers will vary. If the workstation/PC you are using is on the same LAN segment as the Integration Router, you should use the IP address of the Integration Router's LAN port to telnet in. If the Integration Router is across the WAN (i.e., a remote Integration Router), you must use the WAN port IP address of the remote Integration Router.

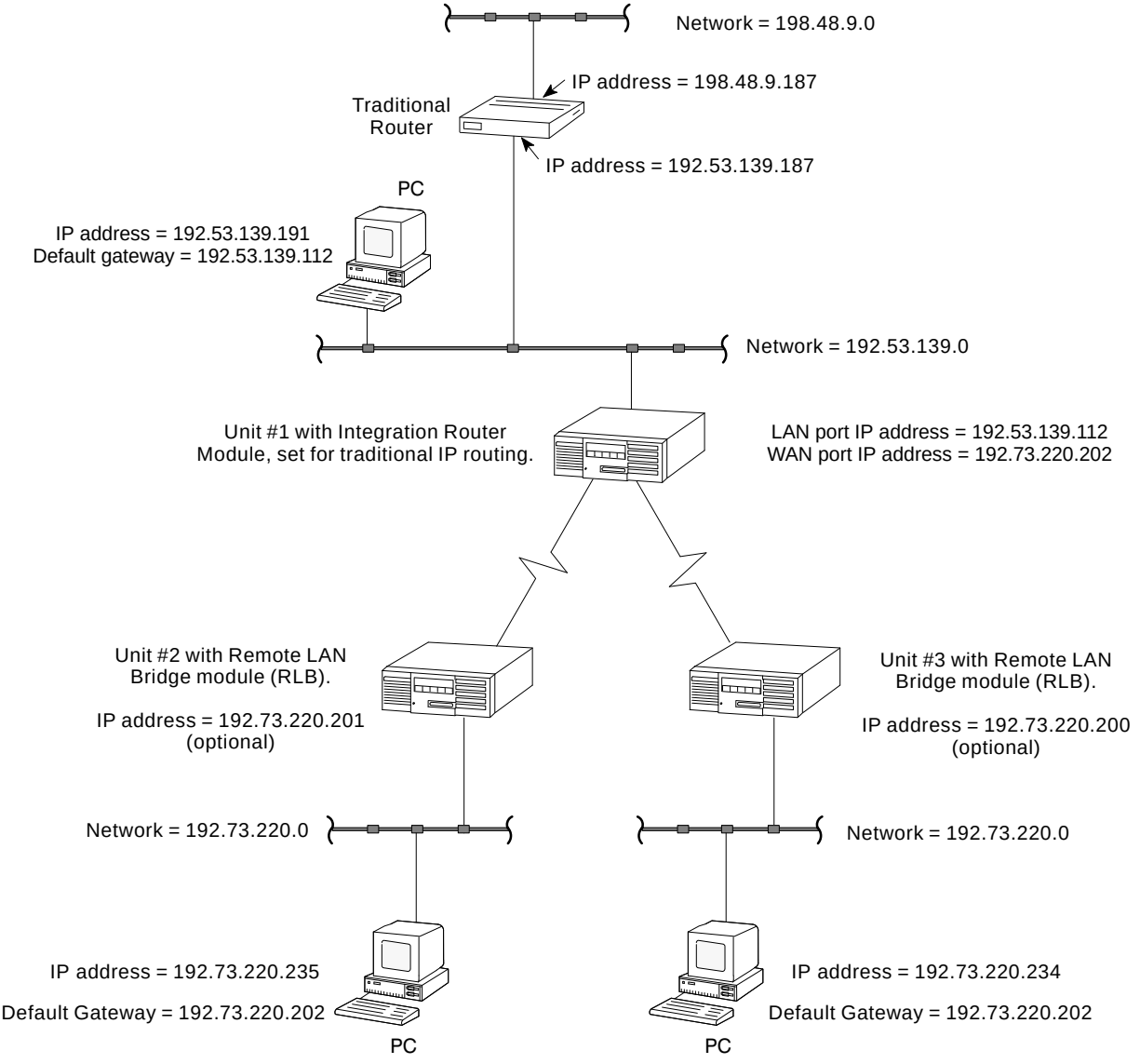
Examples:


Network = 192.1.1.0
Integration Router 1
Router LAN port IP address = 192.1.1.10
Router WAN port IP address = 192.1.4.1
WAN = 192.1.4.0
Router WAN port IP address = 192.1.4.2
Router LAN port IP address = 192.1.2.20
Router WAN port IP address = 192.1.4.3
Router LAN port IP address = 192.1.3.30
Integration Router 2
Integration Router 3
Network = 192.1.2.0
Network = 192.1.3.0
IP address = 192.1.2.2
Default Gateway = 192.1.2.20
PC

- For the PC user to telnet to Integration Router 2, the user would use the IP address of Integration Router 2's LAN port, or, 192.1.2.20. This is because the PC is on the same LAN segment as Integration Router 2.
- For the PC user to telnet to Integration Router 1, the user would use the IP address of Integration Router 1's WAN port, or, 192.1.4.1. This is because Integration Router 1 is located across the WAN from the PC.

Using Integration Routers in IP Routing Mode with Remote LAN Bridges (RLBs)

Here is an example of connecting a unit with an Integration Router set for traditional IP routing, to two units with Remote LAN Bridges.


Network = 198.48.9.0
IP address = 198.48.9.187
Traditional Router
IP address = 192.53.139.187
PC
IP address = 192.53.139.191
Default gateway = 192.53.139.112
Network = 192.53.139.0
Unit #1 with Integration Router Module, set for traditional IP routing.
LAN port IP address = 192.53.139.112
WAN port IP address = 192.73.220.202
Unit #2 with Remote LAN Bridge module (RLB).
IP address = 192.73.220.201 (optional)
Unit #3 with Remote LAN Bridge module (RLB).
IP address = 192.73.220.200 (optional)
Network = 192.73.220.0
Network = 192.73.220.0
IP address = 192.73.220.235
Default Gateway = 192.73.220.202
PC
IP address = 192.73.220.234
Default Gateway = 192.73.220.202
PC

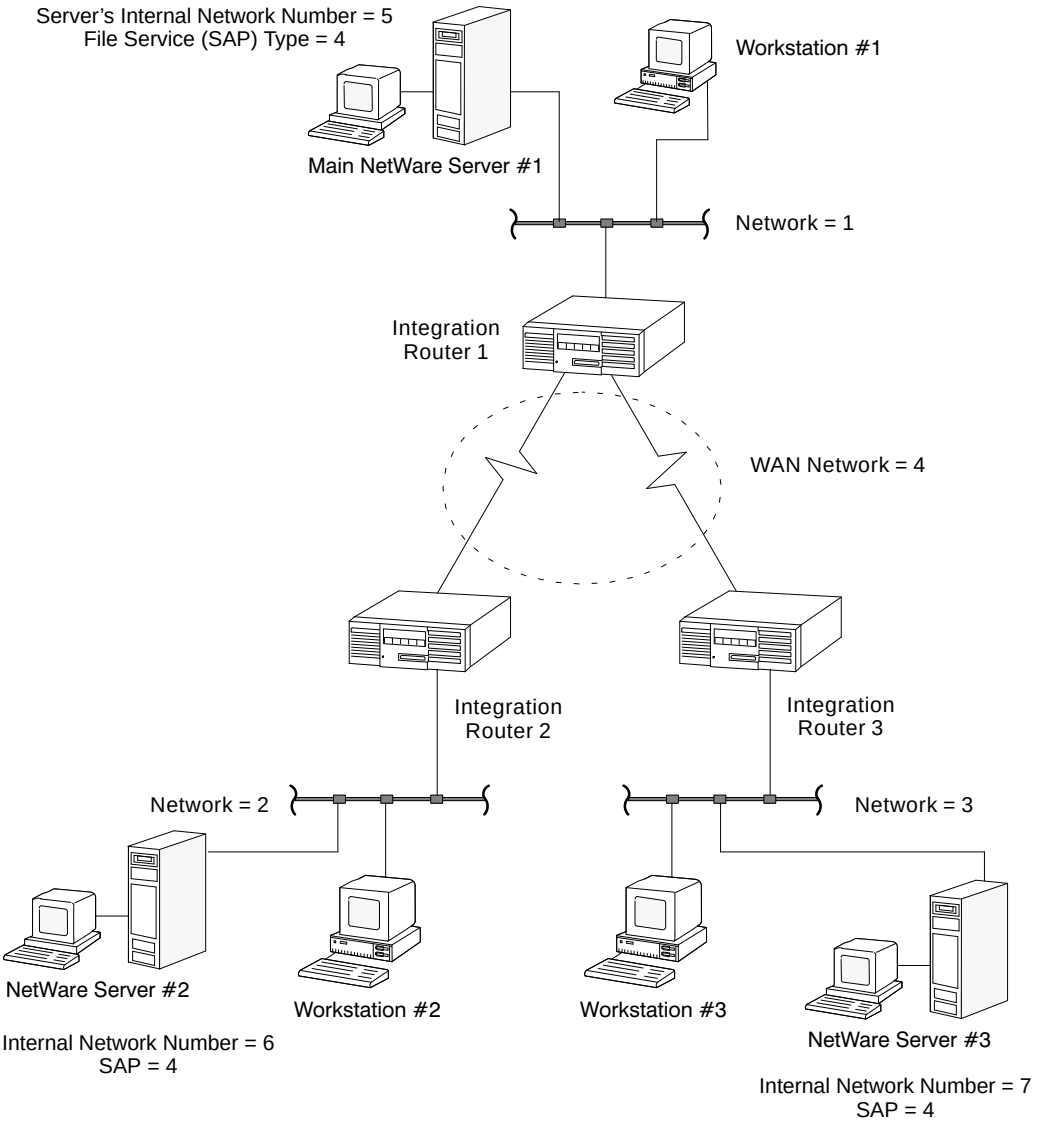
Devices on the Ethernet of the Integration Router (network 192.53.139.0) must have IP addresses in the range 192.53.139.xx (xx = 01 to 235). Devices on the Ethernets of the two Remote LAN Bridges must have IP addresses in the range 192.73.220.xx.

The Ethernet segments of units #2 and #3, plus the WAN of all three units are considered one virtual IP network (192.73.220.0).

All devices on the Ethernet segments of units #2 and #3 should have the default gateway set to 192.73.220.202 (the Integration Router WAN port IP address). If the devices are UNIX machines running the routed daemon (in.routed), which is a RIP process, you don't have to configure the default gateway. Also, if units #2 and #3 have the EasyRouter FEATUREPAK or FlashPak cartridge installed, even though they are running in bridge mode, you don't have to configure the default gateway. This is because the EasyRouter software runs the RIP process even in bridge mode. The command SHOW IP ROUTES will show the routes that RIP has learned.

Filtering IPX SAP Advertisements

The Integration Router can filter specific SAP advertisements. The details and syntax of the various commands to enter filters into the database are described on pages 7-29 to 7-31. The following is an application for using the SAP filters.



In the example network, all file servers have the same SAP type (0004). The following filter is added to Integration Routers 2 and 3:

```
DEFINE IPX GLOBAL SAP_TYPE 04 PORT ETHERNET ADD
```

And, IPX filtering is turned on:

```
DEFINE IPX FILTERING ENABLE
```

The results of adding the filter to Integration Routers 2 and 3 are as follows:

- SAP advertisements from file server 2 are blocked from going to the remote sites. Integration Routers 1 and 3 will never see file server 2. This will prevent file server 1 and file server 3 from accessing file server 2.
- SAP advertisements from file server 3 are blocked from going to the remote sites. Integration Routers 1 and 2 will never see file server 3. This will prevent file server 1 and file server 2 from accessing file server 3.
- Workstations 1 and 2 cannot access file server 3.
- Workstations 1 and 3 cannot access file server 2.
- If workstation 3 is logged into file server 3, the `slist`[1] command will show only these entries:

```
Known NetWare File Servers                    Network   Node Address Status
--------------------------                    -------   ------------ ------
SERVER 3                                     [       7][           1]Default
SERVER 1                                     [       5][           1]

Total of 2 file servers found
```

  Thus, workstation 3 cannot access file server 2 – or any file server in that remote site.

- If workstation 2 is logged into file server 2, the `slist` command will show only these entries:

```
Known NetWare File Servers                    Network   Node Address Status
--------------------------                    -------   ------------ ------
SERVER 2                                     [       6][           1]Default
SERVER 1                                     [       5][           1]

Total of 2 file servers found
```

  Thus, workstation 2 cannot access file server 3 – or any file server in that remote site.

- If workstation 1 is logged into file server 1, the `slist` command will show only this entry:

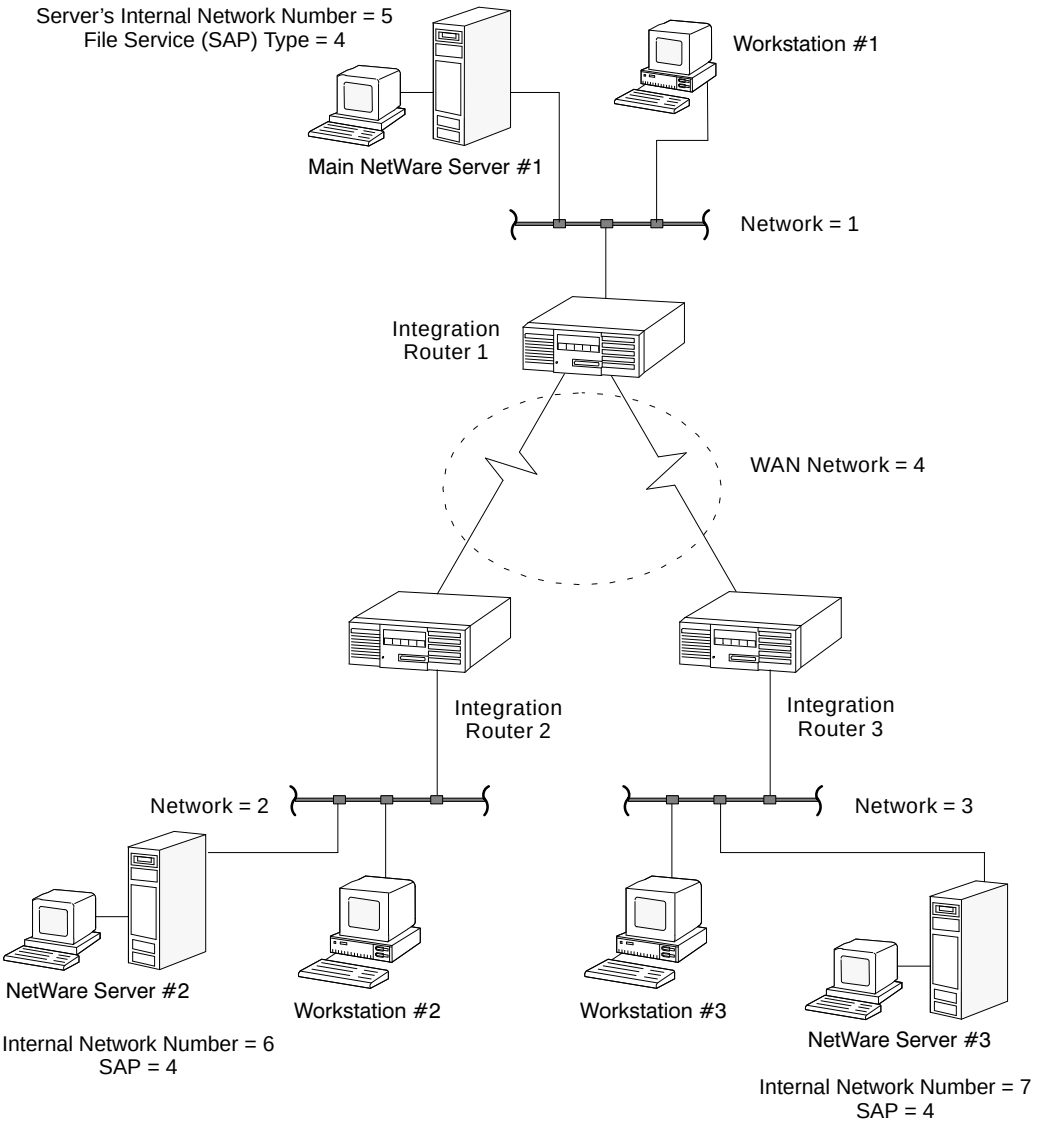
```
Known NetWare File Servers                    Network   Node Address Status
--------------------------                    -------   ------------ ------
SERVER 1                                     [       5][           1]Default
Total of 1 file servers found
```

  Thus, workstation 1 cannot access file server 2 or 3 – or any file servers in the remote sites.

[1] NetWare 386. For NetWare 4.x, the command is `nlist`.

Filtering IPX RIP Advertisements

The Integration Router can filter specific IPX RIP advertisements. The details and syntax of the various commands to enter filters into the database are described on pages 7-29 to 7-31. The following is an application for using the IPX RIP filters.



The following filter set is added to Integration Router 2:

```
DEFINE IPX GLOBAL NETWORK 1 PORT WAN ADD
DEFINE IPX GLOBAL NETWORK 5 PORT WAN ADD
DEFINE IPX GLOBAL NETWORK 6 PORT ETHERNET ADD
DEFINE IPX EXCLUSIVE NETWORK ENABLE
```

And, IPX filtering is turned on:

```
DEFINE IPX FILTERING ENABLE
```

The following filter set is added to Integration Router 3:

```
DEFINE IPX GLOBAL NETWORK 1 PORT WAN ADD
DEFINE IPX GLOBAL NETWORK 5 PORT WAN ADD
DEFINE IPX GLOBAL NETWORK 7 PORT ETHERNET ADD
DEFINE IPX EXCLUSIVE NETWORK ENABLE
```

And, IPX filtering is turned on:

```
DEFINE IPX FILTERING ENABLE
```

The results of adding the filter sets to Integration Routers 2 and 3 are as follows:

- If workstation 3 is logged into file server 3, the `slist`[1] command will show only these entries:

```
Known NetWare File Servers                    Network   Node Address Status
--------------------------                    -------   ------------ ------
SERVER 3                                     [       7][           1]Default
SERVER 1                                     [       5][           1]

Total of 2 file servers found
```

- If workstation 2 is logged into file server 2, the `slist` command will show only these entries:

```
Known NetWare File Servers                    Network   Node Address Status
--------------------------                    -------   ------------ ------
SERVER 2                                     [       6][           1]Default
SERVER 1                                     [       5][           1]

Total of 2 file servers found
```

- If workstation 1 is logged into file server 1, the `slist` command will show only these entries:

```
Known NetWare File Servers                    Network   Node Address Status
--------------------------                    -------   ------------ ------
SERVER 1                                     [       5][           1]Default
SERVER 2                                     [       6][           1]
SERVER 3                                     [       7][           1]

Total of 3 file servers found
```

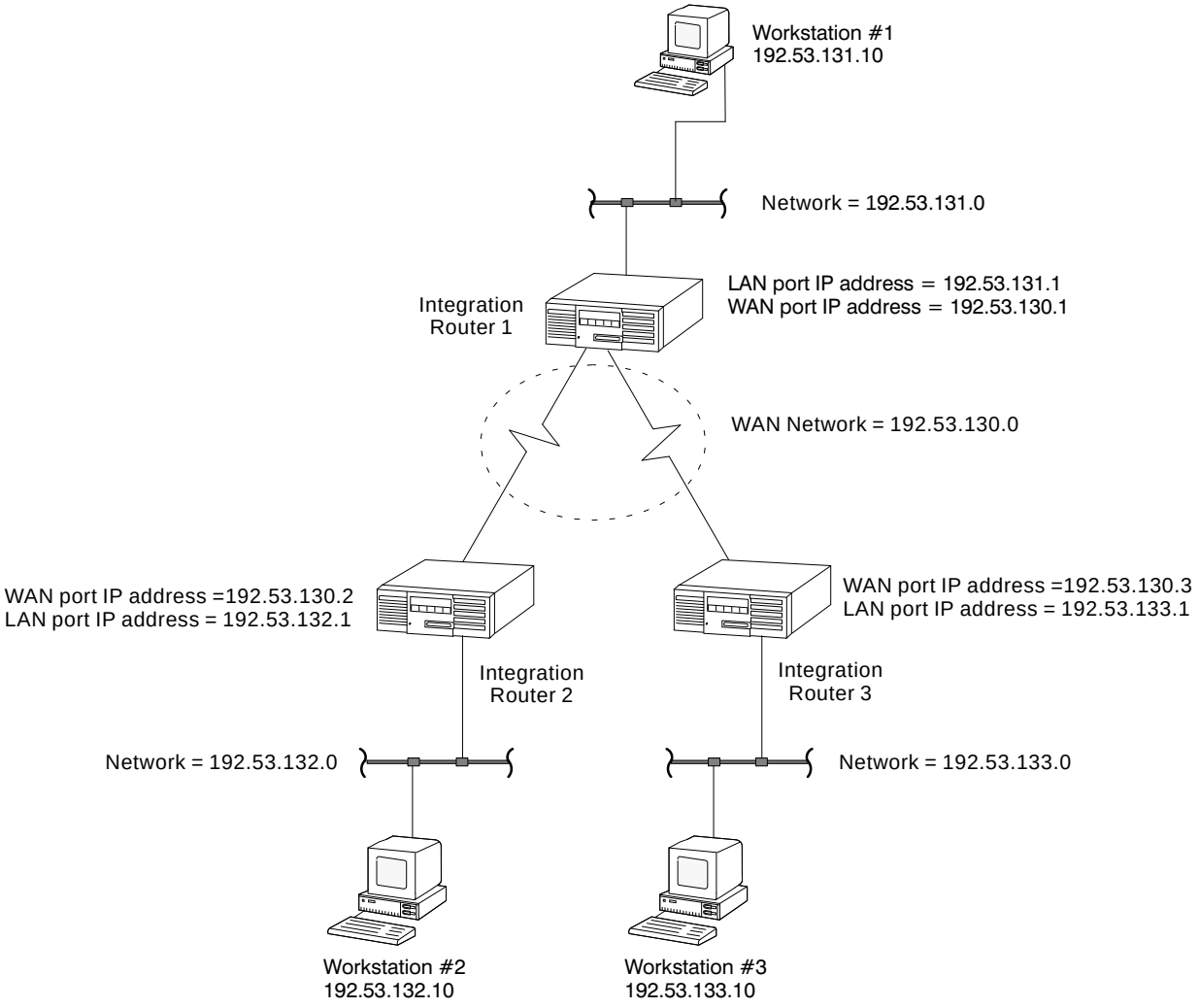
- In brief, the workstations at the remote sites can access their local file servers and the file servers at the main site. The workstations at the main site can access all file servers.

[1] NetWare 386. For NetWare 4.x, the command is `nlist`.

Filtering IP RIP Broadcasts

The IP RIP filters allow you to control the routes that the Integration Router will learn. The details and syntax of the various commands to enter filters into the database are described on pages 7-21 to 7-23.

The following is an example application that uses the IP RIP filters.



For the example network above, the following command sequence is entered at Integration Router 2:

```
DEFINE IP GLOBAL NETWORK 192.53.133.0 ADD
DEFINE IP FILTERING ENABLE
```

And Integration Router 2 is reset.

The following command sequence is entered at Integration Router 3:

```
DEFINE IP GLOBAL NETWORK 192.53.132.0 ADD
DEFINE IP FILTERING ENABLE
```

And Integration Router 3 is reset.

Adding the IP Global Network filters to Integration Routers 2 and 3 will cause the following results:

- The routing table at Integration Router 1 will be as follows (this can be viewed using the SHOW IP ROUTES command):

```
Destination    Gateway       Interf./link   Status  Metric  Type
192.53.131.0   192.53.131.1  ln0       0     Up       0   Static
192.53.130.0   192.53.130.1  wn0       0     Up       0   Static
192.53.132.0   192.53.130.2  wn0       2     Up       1   178
192.53.133.0   192.53.130.0  wn0       1     Up       1   160
```

  The IP workstations on network 192.53.131.0 would be able to access workstations on network 192.53.132.0 and 192.53.133.0.

- The routing table at Integration Router 2 will be as follows:

```
Destination    Gateway       Interf./link   Status  Metric  Type
192.53.132.0   192.53.132.1  ln0       0     Up       0   Static
192.53.130.0   192.53.130.2  wn0       0     Up       0   Static
192.53.131.0   192.53.130.1  wn0       2     Up       1   178
```

  The IP workstations on network 192.53.132.0 would be able to access workstations on network 192.53.131.0, but not access workstations on network 192.53.133.0.

- The routing table at Integration Router 3 will be as follows:

```
Destination    Gateway       Interf./link   Status  Metric  Type
192.53.133.0   192.53.133.1  ln0       0     Up       0   Static
192.53.130.0   192.53.130.3  wn0       0     Up       0   Static
192.53.131.0   192.53.130.1  wn0       1     Up       1   178
```

  The IP workstations on network 192.53.133.0 would be able to access workstations on network 192.53.131.0, but not access workstations on network 192.53.132.0.

The same results can be obtained using the following command sequences:

Integration Router 2:

```
DEFINE IP GLOBAL GATEWAY 192.53.130.3 ADD
DEFINE IP FILTERING ENABLE
```

Integration Router 3:

```
DEFINE IP GLOBAL GATEWAY 192.53.130.2 ADD
DEFINE IP FILTERING ENABLE
```

Network Code Download E

Integration Router 6.0 and subsequent releases are equipped with Flash EPROM. This allows the operating software to be updated without replacing the cartridge. When the operating software has been properly downloaded, the Integration Router will boot up to the new software. If the download is not successful, the Integration Router will keep trying until the download is successful.

The Integration Router can accept the code download from:

- a PC which is connected directly to a CCM asynchronous channel. The PC can then download to Integration Routers anywhere on the WAN. *Alternately*, the PC can download to a remote node using error-correcting modems. When modems are used, the download is restricted to just the Integration Router in the unit to which the PC is connected.
- using Bootp or TFTP from a server on the same LAN as the Integration Router.
- using NETMan release 2.1 or later at a centralized location in the network, to download through a CCM asynchronous channel.

For network code download using NETMan, refer to the NETMan User's Manual (part number 800-1772, latest revision) for the applicable procedures.

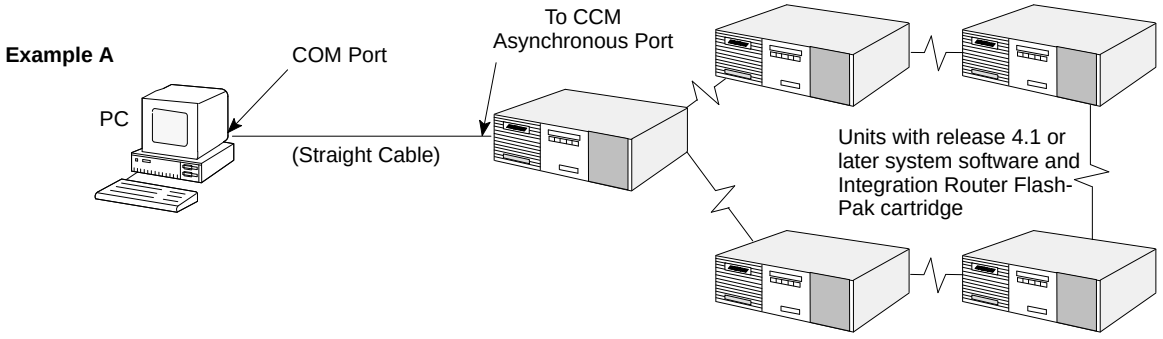
Procedure For Code Download Using A PC

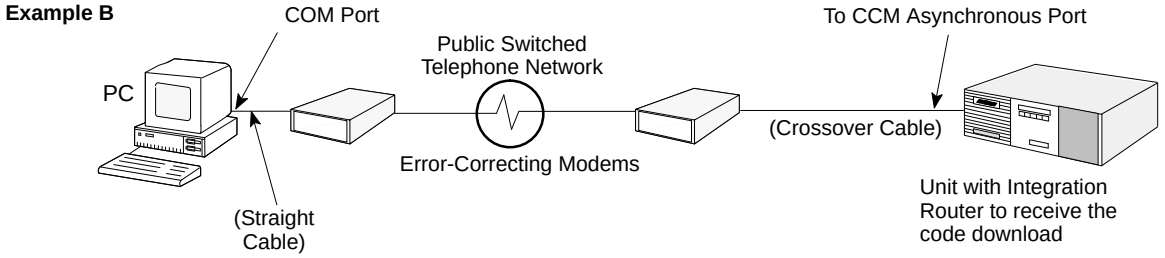
Prerequisites:

- The required minimum PC configuration is:
  - An IBM-compatible, Intel 286-based (or better) PC with:
  - a high-density 3½" floppy drive
  - a hard disk drive
  - an asynchronous COM port
  - Terminal emulation software. We recommend one of the following:
    - PROCOMM PLUS for DOS, version 2.01
    - PROCOMM PLUS for Windows, version 1.02 or 2.0
    - FlashDLD, MICOM's terminal emulation software

  A copy of FlashDLD is included on the diskette labelled *LAN Flash-Pak Code Download Software*. This diskette is packaged with each Integration Router FlashPak cartridge.

- The PC must be connected (directly or using modems) to an asynchronous port of a CCM that has a Release 4.1 or later FEATUREPAK or FlashPak (system, or CCM) cartridge. Here are two examples of how to connect the PC:





- Code to download to the Integration Router. This code is located on the diskette with the following label:

Notes: The FlashDLD program is intended only for downloading software to MICOM products. No other uses for FlashDLD are supported.

MICOM does not support the use of modems with FlashDLD. However, if you do use modems with FlashDLD, they must be error-correcting and modem commands must be entered manually.

The following terminal emulation programs will ***not*** work to download the Integration Router code:

- PROCOMM PLUS for DOS, version 1.1.B or earlier
- PROCOMM PLUS for Windows, version 1.01 or earlier
- The Windows 3.1 Terminal program

1. Install the terminal emulator/file transfer program on the PC.

If you wish to use MICOM's FlashDLD program, then perform either of the following software installation procedures:

To Install FlashDLD for DOS:

Note: This is a simplified installation procedure that should work for most PCs. It is assumed that the 3½" diskette drive is drive A and the software is to be installed on drive C in the default directory to be named FLASHDLD. If you have special requirements, you should refer to the Network Code Download User's Manual (part number 800-1844, latest revision) for more detailed instructions.

a. Place the diskette labelled *LAN FlashPak Code Download Software* into the diskette drive of the PC.

b. Log on to the diskette drive and change directories to the FlashDLD directory:

```
c:\> a:
a:\> cd flashdld
a:\flashdld>
```

c. Enter the *dossetup* command:

```
a:\flashdld> dossetup a
```

The command syntax is: dossetup [source [destination]]. The default destination is C:/FLASHDLD.

d. As dossetup starts up, an Option Selection screen will be displayed. Make sure both FlashDLD Executables and Flash Download Files are selected, then continue with the installation.

The FlashDLD for DOS program will be installed on your PC.

To Install FlashDLD for Windows:

Note: This is a simplified installation procedure that should work for most PCs. It is assumed that the 3½" diskette drive is drive A and the software is to be installed on drive C in the default directory to be named FLASHDLD. If you have special requirements, you should refer to the Network Code Download User's Manual for more detailed instructions.

a. Place the diskette labelled *LAN FlashPak Code Download Software* into the diskette drive of the PC.

b. From the Program Manager, select **File** → **Run**.

In the Command Line box, type the following:

```
a:\flashdld\winsetup.exe
```

Then click on **OK**.

c. When the Setup screen appears, click on **Continue** to proceed with the software installation.

d. In the Destination Path screen, click on **Continue** to select the default software installation directory of c:\flashdld.

e. In the Option Selection screen, make sure both FlashDLD Executables and Flash Download Files are selected, then click on **Continue**.

f. In the Destination Group screen, click on **Continue** to create the default group called FlashDLD.

The FlashDLD for Windows program will be installed on your PC.

2. Start the communications software.

For *FlashDLD for DOS*, at the DOS prompt, enter the following command:

```
c:\flashdld.dos> flashdos
```

For *FlashDLD for Windows*, double click on the FlashDLD for Windows icon.

3. Configure the communications software to the following parameters:

8-bit
No parity
1 stop bit
Hardware or no flow control (do ***not*** select XON/XOFF)
Transparent ASCII or Binary transfer mode
Data rate: same as the port to which the PC is connected (must be either 9600 or 19,200 bps)
COM1 (or whichever PC serial port is connected to the unit)

For *FlashDLD for DOS,* use **Alt-S** to enter the setup mode and **Esc** to exit. When prompted to "Save this configuration?", answer **Y**.

For *FlashDLD for Windows,* select **Configuration** on the menu to enter the setup mode.

Once the communications software has been configured for the code download, set the software to the terminal emulation mode. This is done automatically in FlashDLD, after the configuration has been saved.

4. If modems are used, configure them as follows:

XON/XOFF passthrough
No echo
No result codes
Dial up mode
Asynchronous mode
DCD follows carrier

A suitable command string for Hayes compatible modems would be the following:

```
AT&FE0Q1S0=2S63=1&C1&D0&W
```

5. Configure the local unit's download parameters.

a. Press the Enter key to get the unit's ENTER CLASS prompt:

```
ENTER CLASS:
```

b. Connect to the Command Facility (class $CMD):

```
ENTER CLASS: $cmd
ENTER CLASS PASSWORD
```

c. There are two parameters that affect the Integration Router Network Code Download:

- The password to connect to the unit's $DLD (download) class:

```
COMMAND FACILITY MAIN MENU
   ↓
   CONFIGURE LOCAL NODES
      ↓
      DOWNLOAD PARAMETERS
         ↓
         $DLD PASSWORD
```

  Enter the password for the code download facility ($DLD). The password can have a maximum of 8 characters out of the set of A through Z and 0 through 9. The password is not case-sensitive.

- The inactivity timeout value for the code download:

```
COMMAND FACILITY MAIN MENU
   ↓
   CONFIGURE LOCAL NODES
      ↓
      DOWNLOAD PARAMETERS
         ↓
         $DLD ACTIVITY TIMEOUT
```

  Enter the timeout in seconds. This is the length of time the unit's $DLD facility will wait to disconnect if data transmission has ceased. The default is 120 seconds.

d. Exit the Command Facility:

```
COMMAND FACILITY MAIN MENU
   ↓
   EXIT COMMAND FACILITY
```

6. Place the Integration Router into the code download, WAN-to-LAN mode.

a. Connect to class **node_id/$CMD** (where *node_id* is the name of the unit whose Integration Router is to receive the code download):

```
ENTER CLASS: tpnet/$cmd
ENTER CLASS PASSWORD
```

b. Select **RESET** from the Command Facility Main Menu:

```
COMMAND FACILITY MAIN MENU
   ↓
   RESET
```

c. Select **INTEGRAL LAN** from the Reset Menu:

```
RESET
   ↓
   INTEGRAL LAN
```

d. Specify the slot containing the Integration Router at the `ENTER MODULE LOCATION` prompt:

```
ENTER MODULE LOCATION [B–E] (^X TO ABORT):b
```

e. Select **CODE DOWNLOAD: WAN TO LAN** from the Integral LAN Reset Menu:

```
INTEGRAL LAN RESET
   ↓
   CODE DOWNLOAD: WAN TO LAN
```

You will see a message sequence similar to the following displayed on the screen:

```
21:23:32 TPNET [B] LAN RESET: WAN–>LAN RELOAD
21:24:02 TPNET [B] LAN MODULE UP
21:24:10 TPNET [B] CCM load waiting:
```

You must see the *CCM load waiting:* message displayed before proceeding to the next step. At that point, the Integration Router is in the download mode and ready for data.

7. Exit the Command Facility.

Exit the Command Facility as follows:

a. Select **MAIN MENU** from the Reset Menu:

```
RESET
   ↓
   MAIN MENU
```

b. Select **EXIT COMMAND FACILITY** from the Command Facility Main Menu:

```
COMMAND FACILITY MAIN MENU
      ↓
      EXIT COMMAND FACILITY
```

8. Initiate the code download.

a. Connect to class **node_id/lan_slot/$DLD** (where *node_id* is the name of the unit whose Integration Router is being downloaded and *lan_slot* is the letters LAN plus the module location letter of the module – for example, LANB). An example class connect string would be:

```
ENTER CLASS: tpnet/lanb/$dld
ENTER CLASS PASSWORD
```

b. Enter the password at the ENTER CLASS PASSWORD prompt. You should see the following message sequence:

```
CALL IN PROGRESS
CONNECTED
```

Note: The *CALL IN PROGRESS* message is displayed only if the download is to a remote unit. If the download is to a local unit, only the message *CONNECTED* will be displayed.

IMPORTANT: Do not type in any characters at this point (with the communications software in terminal mode). If text characters are typed in accidentally, the download will fail at the 134K point and the message *CCM bad checksum* will be displayed. The class connect call to $dld will be disconnected. If this happens, restart the download beginning with step 6 (placing Integration Router in the code download mode) of this procedure.

c. Use the Transparent ASCII or Binary file transfer mode of the PC program to send the code download file to the Integration Router.

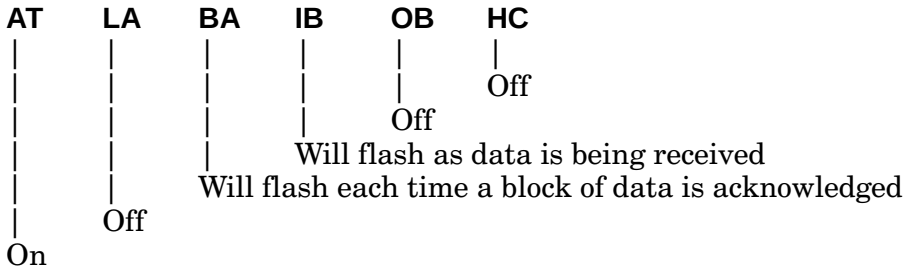
For *FlashDLD for DOS*, enter **Alt-F** to enter the file transfer mode. Then, select the file to download.

For *FlashDLD for Windows,* select **File** → **Send** to enter the file transfer mode. Highlight the file to download, and click on **OK**. Then click on **Send** to initiate the file transfer.

The code download will pause briefly at the 134K point, and then continue until the entire file is transferred. During the download, the Integration Router will cause various messages to be displayed on the LCD (if there is one) and on a $CMD terminal (if connected). On the $CMD terminal, a normal code download will cause the following message sequence:

```
21:24:21 TPNET [B] $DLD Connected.
21:24:53 TPNET [B] CCM downloading...
21:34:01 TPNET [B] CCM load success.
21:34:05 TPNET [B] Adding checksums..
21:34:43 TPNET [B] LAN RESET: VIA LAN MODULE
21:35:05 TPNET [B] LAN MODULE UP
```

The indicators on the LAN module itself will display indications of the code download:



Once the download is successful and the new software stored in the Flash-Pak, the Integration Router will reset and start executing the new software.

If the download is not successful, the reason for the failure will be indicated by the display of one or more of the following messages:

`CCM bad checksum.`
`CCM header fail.`

Text characters were typed in while the communications software was in the terminal mode, which corrupted the header portion of the file transfer. Alternately, the header portion of the download file was not received correctly. Check the download file for integrity and verify that it is the correct file for the Integration Router. Then, reset the unit and restart the download.

`File header read failed.`

The header data received for the code download file was not correct for the Integration Router. Make sure that you have selected the correct download file, then reset the unit and restart the download.

`File load failed, `*`nnnnnn`*` bytes loaded.`

Anytime the code download data transfer started, but did not complete successfully, this message will be displayed. The number of bytes actually transferred will be displayed in the field shown as *nnnnnn* above. The reason for the file load failure will be indicated by other displayed messages.

To reset the unit and restart the download, proceed as follows:

a. (If the Reset Menu is already displayed, skip this step.) At the Command Facility Main Menu, select **RESET**:

```
COMMAND FACILITY MAIN MENU
   ↓
   RESET
```

b. At the Reset Menu, select **NODE**:

```
RESET
   ↓
   NODE
```

c. Enter **Y** to confirm the reset:

```
ENTER "Y" TO CONFIRM OR "N" TO ABORT: Y
```

d. At the Parameter Restoration Menu, select **CURRENT CONFIGURATION**:

```
PARAMETER RESTORATION
   ↓
   CURRENT CONFIGURATION
```

e. When the unit finishes the reset, place the Integration Router into the code download mode, as described beginning with step 6 on page E–6.

Procedures For Code Download Using Bootp or TFTP

IMPORTANT: The server to be used for downloading the Integration Router software must be on the same LAN segment (same network number) as the Integration Router itself. You ***cannot*** perform the download from:

- a server on a LAN segment that is located across the WAN from the Integration Router
- a LAN segment with a different network number that is accessed using a router

The Integration Router can download its operating software from a server running Bootp and TFTP, or TFTP only. Bootp and TFTP download is enabled by default. You must turn off Bootp in order to perform a TFTP only download. Bootp and TFTP are TCP/IP protocols. To perform a code download using these protocols requires some setup on the server. As server configurations vary extensively, the following procedures are only approximate examples. To accomplish this form of code download, you must be experienced in TCP/IP LAN administration. *If you are unsure of how to set up a server to transfer files using Bootp/TFTP, you should perform the code download using a PC connected to a unit on the WAN.*

Code Download Using Bootp/TFTP

Note: The following procedure describes a Sun workstation running SunOS 4.1.3 as the Bootp/TFTP server. Configuring other machine types to be Bootp/TFTP servers may differ in the details, but the essential steps are basically the same.

1. Copy down the hardware address (Ethernet address) of the Integration Router.

a. Connect to class **`node_id/$CMD`** (where *node_id* is the name of the unit whose Integration Router is to receive the code download):

```
ENTER CLASS: tpnet/$cmd
PASSWORD
```

The Command Facility Main Menu should be displayed on your terminal.

b. Select **`INTEGRAL LAN LOCAL MODE ACCESS`** from the Command Facility Main Menu:

```
COMMAND FACILITY MAIN MENU
   ↓
   INTEGRAL LAN LOCAL MODE ACCESS
```

c. Specify the slot containing the Integration Router at the `ENTER MODULE LOCATION` prompt:

```
ENTER MODULE LOCATION [B–E] (^X TO ABORT):b
```

d. At the `Enter username>` prompt, enter a user name:

```
Enter username> Dave
Local>
```

e. Enter the following command:

```
Local> SHOW SERVER
```

f. Copy down the hardware address displayed on the screen.

g. Log out of the Integration Router's command line interface:

```
Local> LOGOUT
```

h. Exit the Command Facility:

```
COMMAND FACILITY MAIN MENU
   ↓
   EXIT COMMAND FACILITY
```

If the PC is connected to an intermediate unit (i.e., not physically connected to the unit whose Integration Router is being downloaded), then exit from that unit's Command Facility Main Menu, as well.

2. Set up the Bootp server that resides on the download host system.

This usually involves the following:

a. Create (or modify) a configuration file that contains information about the devices Bootp is to respond to. This configuration file contains a minimum of the following parameters for each device:

- Hardware (Ethernet) address of the device
- IP address of the device
- Network name of the device
- Name of the file to download to the device

Here is a sample file used in Sun workstations, called /etc/bootptab:

```
micom:ht=1:ha=0040c5010101:ip=199.30.19.214:hd=/tftpboot:bf=MICOMLD.SYS:
micom:ht=1:ha=0040c5100c3f:ip=199.30.19.215:hd=/tftpboot:bf=MICOMLD.SYS:
↑     ↑    ↑               ↑                ↑             ↑
|     |    |               |                |             File to download
|     |    |               |                Directory for download file
|     |    |               Device's IP address in decimal
|     |    Device's hardware address in hexadecimal
|     Device's hardware type (Integration Router = 1)
Network name of the device
```

b. Start the Bootp server process. This may be a specific server process always running on the download host system, or, the server process maybe invoked on an as needed basis (as in the case of Sun workstations). Here is the line for Sun workstations in the /etc/inetd.conf file for starting a Bootp server process:

```
bootps  dgram   udp     wait    root    /etc/bootpd             bootpd
↑       ↑       ↑       ↑       ↑       ↑                       ↑
|       |       |       |       |       |                       Arguments
|       |       |       |       |       Server program
|       |       |       |       User
|       |       |       Wait status
|       |       Protocol
|       Socket type
Service name
```

Once the necessary information is included in the /etc/inetd.conf file, the inetd process is signaled to read the inet.conf file. (Normally, inetd reads the file during server bootup.)

3. Set up the TFTP server that resides on the download host system.

a. Copy the MICOMLD.SYS file from the *LAN FlashPak Code Download Software* diskette to the TFTP directory. For Sun workstations, the default TFTP directory is /tftpboot.

Make sure the TFTP directory and the download file have owner, group, and world read permissions. For example:

```
<root>troll:/> cd /tftpboot
<root>troll:/tftpboot> ls -l
total 2339
drwxrwxrwx  3 root          512 Mar 28 12:51 ./
drwxr-xr-x 21 root         1024 Mar 29 09:03 ../
-rw-rw-r--  1 root       519128 Mar 28 15:27 MICOMLD.SYS
 ↑  ↑  ↑
Owner Read  |  |
            |  |
   Group Read  |
               |
               World Read
```

MICOMLD.SYS is a binary file. You must use the binary mode when transferring this file from the diskette to the download host system.

b. Start the TFTP server process. This may be a specific server process always running on the download host system, or the server process maybe invoked on an as needed basis (as in the case of Sun workstations). Here is the line for Sun workstations in the /etc/inetd.conf file for starting a TFTP server process:

```
tftp    dgram   udp     wait    root    /usr/etc/in.tftpd       in.tftpd –s /tftpboot
↑       ↑       ↑       ↑       ↑       ↑                       ↑
|       |       |       |       |       |                       Arguments
|       |       |       |       |       Server program
|       |       |       |       User
|       |       |       Wait status
|       |       Protocol
|       Socket type
Service name
```

Once the necessary information is included in the /etc/inetd.conf file, the inetd process is signaled to read the inetd.conf file.

Since the –s option (for security) is appended to the in.tftpd argument in the tftp line of the /etc/inetd.conf example above, the TFTP daemon will require the directory to match that specified in the line (/tftpboot). In this case, the /tftpboot directory is expected to be a subdirectory under the default TFTP directory. Thus, it is necessary to create a subdirectory called tftpboot under the /tftpboot directory and set up a link in that subdirectory to the download file in the parent directory. For example:

```
<root>troll:/> cd /tftpboot
<root>troll:/tftpboot> ls –l
total 2339
drwxrwxrwx  3 root          512 Mar 28 12:51 ./
drwxr–xr–x 21 root         1024 Mar 29 09:03 ../
–rw–rw–r––  1 root       519128 Mar 28 15:27 MICOMLD.SYS
drwxrwxr–x  2 root          512 Mar 22 15:42 tftpboot/
<root>troll:/tftpboot> cd tftpboot
<root>troll:/tftpboot/tftpboot> ls –l
total 6
drwxrwxr–x  2 root          512 Mar 22 15:42 ./
drwxrwxrwx  3 root          512 Mar 28 12:51 ../
lrwxrwxrwx  1 root           11 Mar 22 15:42 MICOMLD.SYS –> ../MICOMLD.SYS
<root>troll:/tftpboot/tftpboot>
```

4. Initiate the code download.

a. Connect to class **node_id/$CMD** (where *node_id* is the name of the unit whose Integration Router is to receive the code download):

```
ENTER CLASS: tpnet/$cmd
ENTER CLASS PASSWORD
```

b. Select **RESET** from the Command Facility Main Menu:

```
COMMAND FACILITY MAIN MENU
   ↓
   RESET
```

c. Select **INTEGRAL LAN** from the Reset Menu:

```
RESET
   ↓
   INTEGRAL LAN
```

d. Specify the slot containing the Integration Router at the ENTER MODULE LOCATION prompt:

```
ENTER MODULE LOCATION [B–E] (^X TO ABORT):b
```

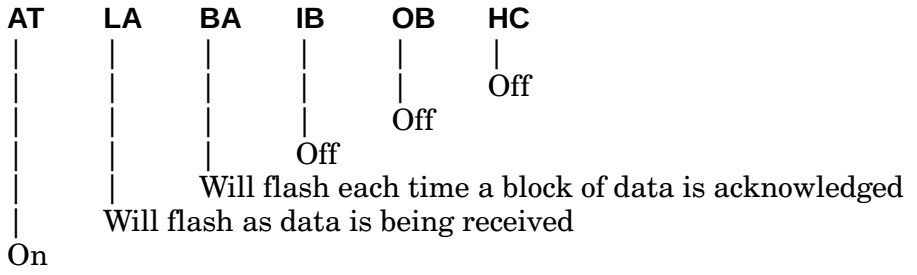
e. Select **CODE DOWNLOAD: LAN TO LAN** from the Integral LAN Reset Menu:

```
INTEGRAL LAN RESET
   ↓
   CODE DOWNLOAD: LAN TO LAN
```

The Integration Router will reset and broadcast a Bootp request to the LAN. It is up to the Bootp server to respond to the Integration Router's Bootp request and initiate the code download. During the download, the Integration Router will cause various messages to be displayed on the LCD (if there is one) and on a $CMD terminal (if connected). On the $CMD terminal, a normal code download will cause the following message sequence:

```
00:05:12 TPNET [B] LAN RESET: LAN->LAN RELOAD
00:05:21 TPNET [B] LAN MODULE UP
00:05:32 TPNET [B] Requesting BOOTP:
00:05:40 TPNET [B] Requesting TFTP:
00:05:55 TPNET [B] TFTP downloading..
00:08:06 TPNET [B] Adding checksums..
00:08:20 TPNET [B] TFTP Load Success
```

The indicators on the LAN module itself will display indications of the code download:



Once the code download is successful, the Integration Router will reset and execute the new code:

```
00:08:26 TPNET [B] LAN RESET: VIA LAN MODULE
00:08:32 TPNET [B] LAN MODULE UP
```

If the download is not successful, the reason for the failure will be indicated by the display of one or more of the following messages:

`File header read failed.`

The header data received for the code download file was not correct for the Integration Router. Make sure that you have selected the correct download file, then reset the Integration Router and restart the download.

`File load failed,` *`nnnnnn`* `bytes loaded.`

Anytime the code download data transfer starts, but does not complete successfully, this message will be displayed. The number of bytes actually transferred will be displayed in the field shown as *nnnnnn* above. The reason for the file load failure will be indicated by other displayed messages.

`No Bootp Reply`

There was no response to the Integration Router's Bootp request broadcast. You should check the Integration Router's LAN connection and ability to reach the Bootp server. The Bootp server must be on the same logical LAN segment as the Integration Router. Also, check the configuration of the Bootp server. The server must be configured correctly in order to respond to Bootp requests. There must be an entry in the server's Bootp configuration file that contains the Integration Router's Ethernet hardware address and includes the information that must be in the Bootp reply (the Internet Address assigned to the Integration Router, the directory path for TFTP downloads, and the name of the code download file). After correcting the source of the problem, reset the Integration Router and restart the download.

`TFTP Access Denied`

The Integration Router does not have permission to access the code download file on the Bootp/TFTP server. Verify that the TFTP directory, the code download file, and the link to the file have owner, group, and world read permissions. Since the Integration Router will automatically continue trying to access the file in order to successfully complete the code download, all you have to do is access the Bootp/TFTP server as superuser and adjust the permissions of the TFTP directory, download file, and link as required. On the next retry of the code download, the Integration Router should be able to access the file and complete the code download without any further intervention.

`TFTP Bad Checksum`

This could be one of two failures:

- The data received was corrupted.
- There was no response to the Integration Router's TFTP GET request by the Bootp/TFTP server.

You should check the Bootp/TFTP server to ensure that it is configured correctly to respond to TFTP requests. Make sure there is an entry in the server's TFTP configuration file that contains the directory for TFTP downloads. After correcting the source of the problem, reset the Integration Router and restart the download.

`TFTP No Such File`

The file that the Integration Router requested to download from the Bootp/TFTP server does not exist. The Integration Router should have received the name and directory path of the file as part of the Bootp/TFTP server's response to the Integration Router's Bootp request. There may be a mismatch between the file name specified in the Bootp configuration file and the file name in the TFTP directory. You should verify the following on the Bootp/TFTP server:

- the Bootp configuration file contains the correct name and directory path of the file that the Integration Router should download,
- the TFTP configuration file specifies the correct directory for the code download file,
- the code download file is present in the TFTP directory and the appropriate permissions and links are set up.

After verifying the configuration of the Bootp/TFTP server, reset the Integration Router, then restart the download.

When using Bootp/TFTP code download, if it is necessary to restart the code download, proceed as follows:

a. (If the Reset Menu is already displayed, skip this step.) At the Command Facility Main Menu, select **RESET**:

```
COMMAND FACILITY MAIN MENU
    ↓
    RESET
```

b. At the Reset Menu, select **INTEGRAL LAN**:

```
RESET
    ↓
    INTEGRAL LAN
```

c. Specify the slot containing the Integration Router:

```
ENTER MODULE LOCATION [B–E] (^X TO ABORT):b
```

d. Select **CURRENT CONFIGURATION** from the Integral LAN Reset Menu:

```
INTEGRAL LAN RESET
    ↓
    CURRENT CONFIGURATION
```

e. When the message LAN MODULE UP is displayed, restart the code download beginning with step 4, *Initiate the code download*, on page E-14.

Code Download Using TFTP

Notes: The following procedure describes a Sun workstation running SunOS 4.1.3 as the TFTP server. Configuring other machine types to be TFTP servers may differ in the details, but the essential steps are basically the same.

If the Integration Router is cold started (reset to factory default values), you will not be able to perform a TFTP–only code download. A cold start will clear all TFTP settings (the IP address of the Integration Router, the IP address of the load host, and the path and file name of the code download file). If the Integration Router has been cold started, you must perform the code download using either Bootp/TFTP, or via a CCM asynchronous port.

1. Assign an IP address to the Integration Router, if it does not already have one.

a. Connect to class **`node_id/$CMD`** (where *node_id* is the name of the unit whose Integration Router is to receive the code download):

```
ENTER CLASS: tpnet/$cmd
PASSWORD
```

The Command Facility Main Menu should be displayed on your terminal.

b. Select **`INTEGRAL LAN LOCAL MODE ACCESS`** from the Command Facility Main Menu:

```
COMMAND FACILITY MAIN MENU
   ↓
   INTEGRAL LAN LOCAL MODE ACCESS
```

c. Specify the module location containing the Integration Router at the `ENTER MODULE LOCATION` prompt:

```
ENTER MODULE LOCATION [B–E] (^X TO ABORT):b
```

d. At the `Enter username>` prompt, enter a user name:

```
Enter username> Dave
Local>
```

e. Enter the following command string at the `Local>` prompt:

```
Local> DEFINE SERVER IPADDRESS ip_address
```

where: *ip_address* is the IP address in decimal, delimited by periods, to be assigned to this Integration Router. An example command would be:

```
DEFINE SERVER IPADDRESS 199.30.19.214
```

2. Configure the Integration Router with the TFTP host's IP address and the path/filename of the download file on the host.

a. Enter the TFTP host's IP address using the following command string:

```
Local> DEFINE SERVER LOADHOST ip_address
```

where: *ip_address* is the IP address of the TFTP host in decimal, delimited by periods. An example command would be:

```
DEFINE SERVER LOADHOST 199.30.19.46
```

b. Enter the directory path and filename of the download file on the TFTP host using the following command string:

```
Local> DEFINE SERVER SOFTWARE /path/filename
```

where: /*path*/ is the directory path on the TFTP host of the download file, and *filename* is the name of the file. The path and filename are case sensitive. The file name extension must be .SYS on the server. However, it is not entered on the DEFINE SERVER SOFTWARE command line. An example command would be:

```
DEFINE SERVER SOFTWARE /tftpboot/MICOMLD
```

3. Set Bootp to DISABLED on the Integration Router using the following command string:

```
Local> DEFINE SERVER BOOTP DISABLED
```

4. Reset the Integration Router to put the TFTP configuration into effect, using the following command string:

```
Local> INITIALIZE SERVER DELAY 0
```

After the Integration Router resets, the Command Facility Main Menu should be displayed on your terminal.

5. Exit the Command Facility.

```
COMMAND FACILITY MAIN MENU
   ↓
   EXIT COMMAND FACILITY
```

If the PC is connected to an intermediate unit (i.e., not physically connected to the unit whose Integration Router is being downloaded), then exit from that unit's Command Facility Main Menu, as well.

6. Set up the TFTP server that resides on the download host system.

a. Copy the MICOMLD.SYS file from the *LAN FlashPak Code Download Software* diskette to the TFTP directory. For Sun workstations, the default TFTP directory is /tftpboot.

Make sure the TFTP directory and the download file have owner, group, and world read permissions. For example:

```
<root>troll:/> cd /tftpboot
<root>troll:/tftpboot> ls -l
total 2339
drwxrwxrwx  3 root          512 Mar 28 12:51 ./
drwxr-xr-x 21 root         1024 Mar 29 09:03 ../
-rw-rw-r--  1 root       519128 Mar 28 15:27 MICOMLD.SYS
 ↑  ↑  ↑
 |  |  |
 |  |  |
 |  |  |
 |  |  World Read
 |  |
 |  Group Read
 |
 Owner Read
```

MICOMLD.SYS is a binary file. You must use the binary mode when transferring this file from the diskette to the download host system.

b. Start the TFTP server process. This may be a specific server process always running on the download host system, or, the server process maybe invoked on an as needed basis (as in the case of Sun workstations).

Here is the line for Sun workstations in the /etc/inetd.conf file for starting a TFTP server process:

```
tftp    dgram   udp     wait    root    /usr/etc/in.tftpd       in.tftpd –s /tftpboot
↑       ↑       ↑       ↑       ↑       ↑                       ↑
|       |       |       |       |       |                       Arguments
|       |       |       |       |       Server program
|       |       |       |       User
|       |       |       Wait status
|       |       Protocol
|       Socket type
Service name
```

Once the necessary information is included in the /etc/inetd.conf file, the inetd process is signaled to read the inetd.conf file.

Since the –s option (for security) is appended to the in.tftpd argument in the tftp line of the /etc/inetd.conf example above, the TFTP daemon will require the directory to match that specified in the line (/tftpboot). In this case, the /tftpboot directory is expected to be a subdirectory under the default TFTP directory. Thus, it is necessary to create a subdirectory called tftpboot under the /tftpboot directory and set up a link in that subdirectory to the download file in the parent directory. For example:

```
<root>troll:/> cd /tftpboot
<root>troll:/tftpboot> ls –l
total 2339
drwxrwxrwx  3 root          512 Mar 28 12:51 ./
drwxr–xr–x 21 root         1024 Mar 29 09:03 ../
–rw–rw–r––  1 root       519128 Mar 28 15:27 MICOMLD.SYS
drwxrwxr–x  2 root          512 Mar 22 15:42 tftpboot/
<root>troll:/tftpboot> cd tftpboot
<root>troll:/tftpboot/tftpboot> ls –l
total 6
drwxrwxr–x  2 root          512 Mar 22 15:42 ./
drwxrwxrwx  3 root          512 Mar 28 12:51 ../
lrwxrwxrwx  1 root           11 Mar 22 15:42 MICOMLD.SYS –> ../MICOMLD.SYS
<root>troll:/tftpboot/tftpboot>
```

7. Initiate the code download.

a. Connect to class **node_id/$CMD** (where *node_id* is the name of the unit whose Integration Router is to receive the code download):

```
ENTER CLASS: tpnet/$cmd
ENTER CLASS PASSWORD
```

b. Select **RESET** from the Command Facility Main Menu:

```
COMMAND FACILITY MAIN MENU
   ↓
   RESET
```

c. Select **INTEGRAL LAN** from the Reset Menu:

```
RESET
   ↓
   INTEGRAL LAN
```

d. Specify the module location of the Integration Router at the ENTER MODULE LOCATION prompt:

```
ENTER MODULE LOCATION [B–E] (^X TO ABORT):b
```

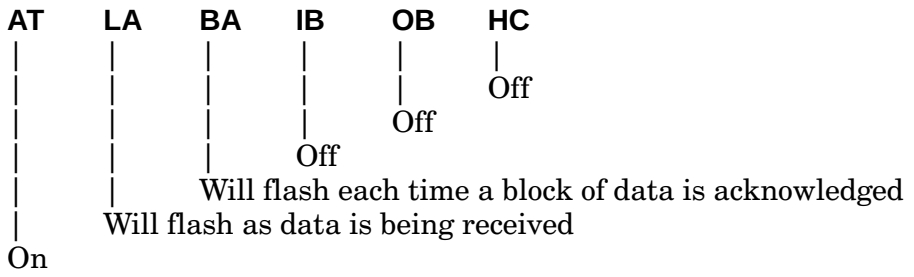
e. Select **CODE DOWNLOAD: LAN TO LAN** from the Integral LAN Reset Menu:

```
INTEGRAL LAN RESET
   ↓
   CODE DOWNLOAD: LAN TO LAN
```

The Integration Router will reset and transmit a TFTP GET request to the download host system. It is up to the TFTP server to respond to the Integration Router's GET request and initiate the code download. During the download, the Integration Router will cause various messages to be displayed on the LCD (if there is one) and on a $CMD terminal (if connected). On the $CMD terminal, a normal code download will cause the following message sequence:

```
00:05:12 TPNET [B] LAN RESET: LAN->LAN RELOAD
00:05:21 TPNET [B] LAN MODULE UP
00:05:40 TPNET [B] Requesting TFTP:
00:05:55 TPNET [B] TFTP downloading..
00:08:06 TPNET [B] Adding checksums..
00:08:20 TPNET [B] TFTP Load Success
```

The indicators on the LAN module itself will display indications of the code download:



Once the code download is successful, the Integration Router will reset and execute the new code:

```
00:08:26 TPNET [B] LAN RESET: VIA LAN MODULE
00:08:32 TPNET [B] LAN MODULE UP
```

If the download is not successful, the reason for the failure will be indicated by the display of one or more of the following messages:

`File header read failed.`

The header data received for the code download file was not correct for the Integration Router. Make sure that you have selected the correct download file, then reset the Integration Router and restart the download.

`File load failed,` *`nnnnnn`* `bytes loaded.`

Anytime the code download data transfer starts, but does not complete successfully, this message will be displayed. The number of bytes actually transferred will be displayed in the field shown as *nnnnnn* above. The reason for the file load failure will be indicated by other displayed messages.

`TFTP Access Denied`

The Integration Router does not have permission to access the code download file on the TFTP server. Verify that the TFTP directory, the code download file, and the link to the file have owner, group, and world read permissions. Since the Integration Router will automatically continue trying to access the file in order to successfully complete the code download, all you have to do is access the TFTP server as superuser and adjust the permissions of the TFTP directory, download file, and link as required. On the next retry of the code download, the Integration Router should be able to access the file and complete the code download without any further intervention.

`TFTP Bad Checksum`

This could be one of two failures:

- The data received was corrupted.
- There was no response to the Integration Router's TFTP GET request by the TFTP server.

You should check the Integration Router's LAN connection and ability to reach the TFTP server. The server must be on the same logical LAN segment as the Integration Router. Also, check the configuration of the TFTP server. The server must be configured correctly in order to respond to TFTP requests. There must be an entry in the server's TFTP configuration file that contains the directory for TFTP downloads. After correcting the source of the problem, reset the Integration Router and restart the download.

`TFTP No Such File`

The file that the Integration Router requested to download from the TFTP server does not exist. Make sure you have entered the correct directory and filename using the DEFINE SERVER SOFTWARE command. Also, you should verify the following on the TFTP server:

- the TFTP configuration file specifies the correct directory for the code download file,
- the code download file is present in the TFTP directory and the appropriate permissions and links are set up.

After verifying the configuration of the Integration Router and TFTP server, reset the Integration Router, then restart the download.

When using TFTP code download, if it is necessary to restart the code download, proceed as follows:

a. (If the Reset Menu is already displayed, skip this step.) At the Command Facility Main Menu, select **RESET**:

```
COMMAND FACILITY MAIN MENU
   ↓
   RESET
```

b. At the Reset Menu, select **INTEGRAL LAN**:

```
RESET
   ↓
   INTEGRAL LAN
```

c. Specify the slot containing the Integration Router:

```
ENTER MODULE LOCATION [B-E] (^X TO ABORT):b
```

d. Select **CURRENT CONFIGURATION** from the Integral LAN Reset Menu:

```
INTEGRAL LAN RESET
   ↓
   CURRENT CONFIGURATION
```

e. When the message LAN MODULE UP is displayed, restart the code download beginning with step 7, *Initiate the code download*, on page E-21.

Glossary

AppleTalk

Allows networking among Macintosh computers. All Macintoshes have a LocalTalk port, running AppleTalk over a 230 kbit serial line. AppleTalk also runs over Ethernet (EtherTalk) and Token Ring (TokenTalk) network media. Due to dynamic addressing and powerful name directory services, installing an AppleTalk device is generally as simple as attaching it and turning it on.

ARP, Address Resolution Protocol

A network protocol that allows hosts to discover a node's hardware address from its IP address. ARP requests are generally sent as broadcasts to all nodes, and the node whose IP address matches that in the request replies. The ARP command on UNIX hosts displays and modifies the IP-to-hardware address translation tables.

AUI, Attachment Unit Interface

A 15-pin D-connector interface used to connect the LAN module to a transceiver. See *MAU*.

backbone

Any LAN has a main "cable" – the main path over which the majority of LAN traffic is routed. ("Cable" is misleading because LANs can be over radio frequency, microwave, or fiber optic carriers.) For example, in a university campus setting, the backbone might be the cable that runs to all the buildings that need network access. Local sub-networks and devices are attached off the backbone.

BNC connector

A connector for ThinNet LAN cables. The connection to the BNC connector on most devices will usually be a BNC T-adapter.

Bootp, Bootstrap Protocol

A protocol, included in the TCP/IP protocol set, that allows a client device to download its IP address and subnet mask, the address of a server host, and a filename from a server on the LAN. This protocol is generally used to boot diskless nodes (the downloaded file is the nodes' operating system that is loaded into memory and executed). However, for the Integration Router, this protocol is used to download information which is used by TFTP to download new operating software into the FlashPak cartridge.

bridge

Connects together two or more LANs of the same access method and general location. A bridge works at the OSI Medium Access Control layer and is transparent to upper-layer devices and protocols. A *local bridge* connects LANs at one location. A *remote bridge* connects LANs that are separated by a significant distance. This is done using a WAN link.

broadcast

The transmission of a message intended for all stations on a network rather than for a specific station.

broadcast storm

Network congestion because of large numbers of frames transmitted by many stations in response to a transmission by one station.

CCM

The Communications Control Module containing the FEATUREPAK/ FlashPak cartridge and providing control of channel communication.

cluster

A group of units which have been assigned the same name. A means of organizing the network to reduce traffic over the WAN link.

compression

The use of statistical methods to reduce the number of bits transmitted across a WAN link.

datagram

An information packet that includes the destination address provided by the user, not the network, along with whatever data the packet carries.

DNS, Domain Name Server

A server that can translate a symbolic name (for example, dave) into an IP address (for example, 192.53.139.200).

domain

A group of nodes on a network that has been assigned a symbolic name.

downline loading

The process of sending configuration parameters or operating software from a controlling device to another device.

fan-out transceiver

A transceiver that uses only one tap on a backbone cable, yet provides the equivalent of multiple transceivers for devices to connect to. A transceiver with multiple inputs and one output. Also known as multiport transceiver.

filter

A bridge feature that compares each received packet with specifications set by the user to either forward or reject it.

FTP, File Transfer Protocol

A TCP service that provides a method of transferring files between computers on a network.

gateway

A server that can access two or more different networks. As such, it can forward messages across networks that other hosts would not be able to access. The gateway generally has multiple IP addresses (one for each network). For example, a gateway might "live" at addresses 192.6.7.8 and 193.6.7.8. Hosts wishing to forward messages address the messages to the gateway, which will then pass them on to the other network.

hardware address

See *network address*.

host

Host is generally used in this manual to mean a node (computer) on a network that can be used interactively, i.e., logged in to.

ICMP, Internet Control Message Protocol

ICMP messages are sent by TCP/IP nodes in response to errors in TCP/IP messages or queries from other nodes. They are sent, for example, when a node sends a packet to an incorrect gateway server, or if a network packet expires. ICMP messages may also be sent as broadcasts, not just sent to a specific host.

interconnect link

See *WAN link*.

Internet

A collection of TCP/IP world-wide networks and gateways, including ARPAnet, MILnet, and NSFnet.

IP Address

See *network address*.

IPX, Internet Packet Exchange

Novell NetWare's native LAN communications protocol.

jumper

A miniature connector that fits over, and electrically connects two pins.

LAT, Local Area Transport

A Digital Equipment Corporation proprietary network communication protocol. The protocol is based on the idea of a relatively small, known number of hosts on a local network sending small network packets at regular intervals. LAT will not work on a wide area network scale, as TCP/IP does, because it cannot distinguish large numbers of nodes. For local networks, however, LAT is usually faster and less prone to pauses than TCP/IP. It also allows remote connections to LAT services and other local area network devices of which TCP/IP has no understanding.

latency

The amount of time it takes for a discrete event to occur.

link

A communications circuit or transmission path connecting multiple points in a network. In MICOM products, an *interconnect link* connects two units over a leased line using an analog or digital circuit provided by the telephone company.

MAC, Medium Access Control

The layer in between the physical and datalink layers that controls the use of network hardware.

MAU, Medium Attachment Unit

A small device used as a transceiver between a network cable and an AUI port. It consists of the physical adapter as well as the circuitry needed to convert signals from one medium to the other.

MIB, Management Information Base

A tree-structured database of management information stored within the internal memory of a LAN device that is configured with an SNMP agent. MIB includes data such as the type of available information and where this information can be found.

module

A printed circuit board and components with specific functionality that plug into one of the module locations in a unit.

module location

One of the slots on a unit which accept modules. These are identified from bottom to top with letters.

MOP, Maintenance Operations Protocol

A DEC protocol for Ethernet traffic. It is used for remote communications between hosts and devices on the network. MOP is also used to signal the server of an NCP request or connection from another host.

multicast

A message that is sent out to a group of nodes by a host. Multicasts are generally sent at specified intervals to avoid cluttering the network, and contain the name of the host sending them as well as information about what services that host provides.

nameserver

For telnet and rlogin connections, the host to connect to can be specified one of two ways – either as a text name, such as alex.weasel.citco.com, or as a numeric IP address (such as 195.22.89.172). The latter form can be routed easily, since hosts on the network know how to map numeric addresses to exact hosts. They have more trouble with names, however, and this is where nameservers come in. Some host(s) on the network are designated as nameservers, to translate (or resolve) text-style names into numeric addresses. No telnet connect request can be transmitted until a numeric address is known for a host, so if there is no accessible nameserver to provide information on hosts not found in the local host table, numeric addresses must be used. Same as *Domain Name Server*.

NCP, Network Control Program

A program running on VMS equipment that allows system managers to configure their local network hardware and remote network devices. In the case of the Integration Router, NCP can be used to remotely log in to the Integration Router to configure those parameters that are configurable from the command line.

NETMan

A MICOM UNIX-based network management system.

NetBIOS, Network Basic Input/Output System

IBM network layer linking operating systems with specific hardware using the OSI Transport Layer.

NetWare

A Novell-developed Network Operating System. Provides file and printer sharing among networks of personal computers. Each NetWare network must have at least one fileserver, and access to other resources is dependent on connecting to and logging into the fileserver. The fileserver(s) control user logins and access to other network clients, such as user PCs, print servers, modem/fax servers, disk/file servers, etc.

network address

Every node on an Ethernet network has one or more addresses associated with it.

Every node has what is called a *hardware address* that is unique across every network everywhere, at any time. If you know a node's hardware address, you should be able to identify the exact piece of equipment it goes with. Hardware addresses are generally set up by the company that manufactured the equipment and should never change. This address is usually specified as a list of six hexadecimal numbers separated by dashes, such as ae-34-2c-1d-69-f1. The hardware address for the LAN module is shown on a label on the back panel of the module.

In the case of TCP/IP networks, each node also has a *software* or "IP" address. This is configurable by the network administrators of the nodes. The software address is usually specified as four decimal numbers separated by periods (for example, 197.49.155.247). In this case, each number must be between 0 and 255, and each segment of the number corresponds to a different network or sub-network. Depending on how many other nodes and networks a node can "see" on its network, addresses are either assigned to nodes (in the case of large, cross-country networks) or chosen randomly (for a small network that does not connect to the outside world). Each software address should be unique.

node

Any intelligent device physically connected to the network. For the LAN, this includes terminal servers, host computers, and any directly connected hardware devices, such as printers and terminals that run off the network. A LAN node can be thought of as any device that has a *hardware address* (see *network address*). A "service node" is a node on the LAN that provides a service other users can connect to (a printer, for example). A terminal server that allows only local logins, on the other hand, is not a service node, as remote users are not allowed to connect to it.

octet

A sequence of eight bits operated on or considered as a unit.

OSI model, Open Systems Interconnection model

An idealistic, seven-layer hierarchical reference structure for defining, specifying, and relating communications protocols. In the model, groups of communications protocols are arranged in layers. The first four (physical, data link, network, and transport) are concerned with transmission and routing. The last three (session, presentation, and application) are concerned with user applications.

OSPF, Open Shortest Path First

A routing protocol that enables routers to make decisions based on traffic load, circuit cost, and service priority from origin to destination.

PING, Packet InterNet Groper

A method of testing the accessibility of a destination by sending an ICMP echo request and then waiting for a reply.

port

Generally refers to a hardware connector through which other devices can be physically connected to a computer unit.

protocol

Any standard method of communicating over a network. There are protocols for placing actual bits onto the network cable; other protocols are layered on top from there.

RARP, Reverse Address Resolution Protocol

A method by which a node can find its IP address using its hardware address. The node broadcasts an RARP request that contains the physical address and a RARP server will respond with the IP address.

RIP, Routing Information Protocol

Within IP networks, RIP is an interior gateway protocol used by routers and host systems to exchange information about reachable networks. RIP uses a distance–vectoring algorithm to establish and maintain network routes.

Within IPX networks, RIP is a dynamic routing protocol used by routers and host systems to gather and maintain information about the network. IPX host systems use RIP requests to determine the network number they are connected to or to find out the route to a network. A router or another IPX host can respond to RIP requests. Routers periodically broadcast the information in their routing table using RIP.

rlogin

An application that provides a terminal interface between (usually UNIX) hosts using the TCP/IP network protocol. Unlike telnet, rlogin assumes the remote host is (or behaves like) a UNIX machine. Rlogin can also be configured to disable login password checking, so it should be used with care. See your host documentation (especially regarding the .rhosts and hosts.equiv files) for more information.

router

A device that looks at a packet's destination address to determine which network is its destination. The router will then find the best path to use to send the packet across the network(s). Routers operate at the Network layer of the OSI reference model.

SAP, Service Advertising Protocol

File servers and application programs in IPX networks periodically advertise their availability and names to clients on IPX networks using SAP. Also, clients send SAP requests to ask for the translation of an advertised service name to a socket on a specific node in the network.

server

A network node that provides services to other nodes on the network. Servers provide printer access and spooling, file access, gateways, etc.

SNMP, Simple Network Management Protocol

A widely used network management protocol that allows network administrators to monitor, troubleshoot, and control other SNMP-compliant devices attached to the network.

subnet

A means of splitting IP addresses into two fields to separate packets for local destinations from packets intended for remote destinations. This makes small networks more efficient.

subnet mask

When looking at an IP packet, the Integration Router must decide whether the packet's destination is for a node on the local network (and can be accessed directly) or whether the destination is a node on a remote network (and must be accessed through a gateway). It does this with the subnet mask set up for the gateway server. The Integration Router uses the mask as a filter; if the Integration Router IP address and the destination IP address appear the same after the filter, the destination node is assumed to be on the same local network. Otherwise, the gateway is used. The mask itself is a list of bits that should be enabled in the result – a 1 in the mask means to let that bit in the IP address through, and 0 means do not. If the subnet mask is not set explicitly, the Integration Router will assume a mask based on its IP address (and thus the apparent network type). This mask will be 255.255.255.0 for most IP addresses.

tap

Refers to a point on the backbone cable where devices can be attached. Taps may be of several types, including BNC "T" connectors, or "vampire" taps that attach directly to a network cable.

TCP/IP, Transmission Control Protocol/Internet Protocol

This is a network protocol set. TCP/IP is extremely flexible, allowing reliable access to over four billion possible nodes anywhere in the world. It also allows many applications to run on top of it. The protocol set usually includes telnet and FTP, and sometimes includes rlogin. TCP/IP support may be integral to an operating system, as in UNIX, or it can be a separate product.

IP is the low level protocol for the TCP/IP protocol set. IP provides packet delivery services between nodes. On the same level as IP are ARP and RARP.

TCP is a reliable stream-delivery, virtual circuit connection-oriented protocol that runs on top of IP. Telnet, FTP, and rlogin use TCP connections.

telnet

An application that provides a terminal interface between nodes using the TCP/IP network protocol. It has been standardized so that "telnetting" to any host should give you an interactive terminal session, regardless of the remote host type or operating system.

TFTP, Trivial File Transfer Protocol

A simple protocol used to transfer files between machines. Its only purpose is to read and write files from or to a remote server. It is distinguished from other file transfer protocols in that TFTP cannot list directories and has no provision for user authentication.

ThickNet

IEEE 802.3 ½-inch diameter coaxial cable. It is generally found on larger networks where a cable may travel for long distances and usually connects multi-user computers to the network. It is harder to work with than ThinNet cable, but offers better noise and error protection and can be run much farther (up to 500 meters/1500 feet without repeaters) than the thin version. ThickNet is also referred to as ThickWire and 10Base5.

ThinNet

IEEE 802.3 thin coaxial cable (RG-58) similar to that used for television/video hookups and typically used with BNC-type connectors. ThinNet is much easier to route and work with than ThickNet, but it should not be run more than 185 meters (about 600 feet) without using a repeater to reinforce the signal. ThinNet connectors are frequently seen on terminal servers, personal workstations, networked printers, and in networks where the nodes are all relatively close to each other. ThinNet is also referred to as ThinWire, CheaperNet, and 10Base2. ThinWire is a trademark of Digital Equipment Corporation.

transceiver

The actual device that interfaces between the network and the local node. When talking about networks, the term transceiver generally refers to any device that actively converts signals between the network and the local node. An example of a transceiver is a MAU.

UDP, User Datagram Protocol

An "unreliable" connectionless protocol. "Unreliable" simply means that there is no verification that packets reached their destination. However, the process is sufficient to allow an application on one node to communicate with a process on another machine.

unit

A unit is any MICOM Integration product, such as a Marathon, NetRunner, etc.

unshielded twisted pair

A LAN that uses two pairs of twisted, unshielded wires to connect a node to a device called a hub. The wiring is similar to that used for telephone sets. The hub can connect several nodes (usually 8 or 12) to the backbone. Unshielded twisted pair LANs are not used as backbones. Unshielded twisted pair is also referred to as UTP and 10BaseT.

WAN link

This is known as the interconnect link in the software. It is the link that connects Integration units together.

INDEX

Numbers

10BaseT, 2-5, 3-1

A

Access Command Mode, 7-1
Active Port Discovery, B-5
Address Table, 3-2, 4-8, 7-10
Agencies
  BABT, ii, iii
  CSA, ii
  FCC, ii
  TÜV, iii
  UL, iii
Allocation Failure, 7-48
ANSI Terminals, 7-49, 7-52
AppleTalk, 7-13, 7-14
Applications
  multi-site, 4-3
  point-to-point, 4-2
ARP, 7-5–7-7, 7-13, 7-16, 7-26
  spoofing, 1-5, 1-6, 7-6–7-8, 7-15–7-17, 7-19–7-22
AUI Connector, 2-1, 2-2, 2-5, 2-6, 3-1, 7-38, A-1, B-1, B-5, Glossary-1

B

BABT, B-2
Backbone network, Glossary-1
Bad Network Number, 7-28, 7-32
Battery, A-2, B-1
  See also Lithium Battery
BNC Connectors, 2-7, Glossary-1
Boot-up, 3-2
Bootp, 5-2, 7-37, Glossary-1
BPDU Packets, 4-11, 7-17
Bridge, 7-5–7-20
  configuration, viewing, 7-19
  definition, 1-12
  identifier, 4-11
  mode, 3-7
  protocols, A-1
  state, setting, 7-10
  traffic statistics, 7-20
Broadcast, 1-3, 1-5, 1-7, 7-7, 7-38
  identification string, 7-38
  reduction, A-1
  storm, 1-3, 1-5, 1-7

C

Clear Screen, 7-49
CLS, 7-49
Cluster, 1-12, 2-2, 2-3, 4-3–4-6, 7-7, 7-18
  assigning unit to, 4-6, 7-7
  communication between, 4-6
  for network security, 4-6
  for routing, 5-1
  name, 2-3, 4-4, 4-6, 7-7
Collision, 7-45, 7-47
Command Mode, accessing, 7-1
Command Port, 7-49, 7-55
Commands, 7-1–7-2
  bridge
    addresses, 7-15
    ARPBcast filtering, 7-5
    ARPBlock, 7-15
    ARPCache, 7-16
    ARPSpoof, 7-6
    ARPSpoof blocking thold, 7-6
    ARPSpoof blocking timer, 7-6
    ARPSpoof cache_timeout, 7-7
    broadcast, 7-7
    cluster, 7-7
    compression, 7-8
    counters, 7-16
    exclusive, 7-12
    global, 7-13
    multicast, 7-8
    nodes, 7-18
    SAPSpoof, 7-9
    SAPSpoof blocking thold, 7-9
    SAPSpoof blocking timer, 7-9
    span, 7-10
    specific, 7-14
    state, 7-10
    status, 7-19
    traffic, 7-20
    weed, 7-10

Commands (cont'd)
General, 7-49–7-55
CLS, 7-49
connect WAN, 7-49
finger, 7-49
help, 7-49
initialize server, 7-50
lo, 7-50
lock, 7-50
logout, 7-50
man, 7-50
ping, 7-51
purge sysdump, 7-51
save, 7-51
set ports, 7-52
set privileged, 7-52
show ports, 7-53
su, 7-54
sysdump, 7-54
test, 7-55
unlock port, 7-55
users, 7-54
WAN, 7-55
who, 7-55
zero counters, 7-55
IP, 7-21–7-25
ARP, 7-26
counters, 7-26
exclusive gateway, 7-21
exclusive network, 7-21
filtering, 7-22
global gateway, 7-22
global network, 7-23
RIP, 7-23
routes, 7-27
routing, 7-23
static, 7-24
static default, 7-24
WAN IPaddress, 7-25
WAN subnet mask, 7-25
IPX, 7-28–7-33
Ethernet frame_type, 7-28
Ethernet network number, 7-28
exclusive network, 7-29
exclusive SAP_type, 7-29
filtering, 7-29
global network, 7-30
global SAP_type, 7-31
routing, 7-32
WAN network number, 7-32
WAN optimize, 7-33
server, 7-37–7-47
announcements, 7-37
characteristics, 7-44
circuit timer, 7-37
counters, 7-45
domain, 7-38
Ethernet, 7-38
identification, 7-38
incoming, 7-39
IPaddress, 7-39
lock, 7-40
login password, 7-40
maintenance password, 7-40
multicast timer, 7-41
name, 7-41
nameserver, 7-41
number, 7-41
password limit, 7-42
privileged password, 7-42
prompt, 7-42
retransmit limit, 7-43
status, 7-48
subnet mask, 7-43
Compatibility, 1-9
Compression, 7-17, 7-19, A-2
hardware/software, 7-8
Connect
to LAN, 2-5–2-8
to WAN, 7-49, 7-55
Connect Failure, 7-47
Connect WAN, 7-49
Conventions, 1-9, 1-12
Counters, 7-16, 7-26, 7-34, 7-45, 7-54
CSA, B-2
Customer Service, v

D

Data Compression, 7-17, A-2
DB15. *See* AUI Connector
DECnet, 7-13, 7-14
Define, 7-5
Delta Update, 6-1
Device (definition), 1-12
DNS (Domain Name Server), 5-2
Dump, 7-51, 7-54
Dynamic Routes, 7-27

E

EasyRouter
  FlashPak cartridge, 1-13
  mode, 2-2, 3-4, 3-7
  technology, 1-3, A-1
Error Codes, 7-46, 7-47
Ethernet Activity, 7-16
Ethernet Address. *See* Hardware Address
Ethernet Frame_Type, 7-28
Ethernet Interface, A-1
Exclusive Filter Mode, 4-10, 7-11, 7-12

F

Fan-out Transceiver, 2-8
FEATUREPAK/FlashPak Cartridge, 1-12, 2-1
Filter, 4-7–4-10, 7-11–7-14, 7-17, 7-19
  destination address, 4-7, 4-8
  exclusive mode, 4-10
  global, 7-11–7-13, 7-19–7-21
  hierarchy, 4-9
  pattern, 4-10, 7-13, 7-14
  performance, A-2
  protocol, 4-10, 7-13, 7-14
  specific, 7-11, 7-12, 7-14, 7-20
  static address, 4-9
Finger, 7-49
FlashPak Cartridge, B-3, B-4
Frame Type, 7-28

G

Gateway, 5-1, 7-24, 7-38, 7-43
Gateway host, Glossary-3
Global Filter, 7-11–7-13
Guard Bracket, B-4

H

Hardware Address, 2-2, 4-9, 7-15, B-1
Hardware Compression, 7-8
Hardware Port Selection. *See* Port, selection
Help, 7-49, 7-50
Host, Glossary-3

I

IEEE 802.1D, A-2
IEEE 802.3, 2-1, 2-5, 2-8, A-1
Indicators, 3-3
Initial Setup, 3-4
Initialize Server, 7-50
Installing
  FlashPak cartridge, B-3, B-4
  LAN module, B-1–B-5
Interconnect Link. *See* WAN Link
Interoperation With Traditional Routers, 4-12
Invalid Packet, 7-46, 7-47
IP, 1-3, 5-1, A-1
  address, 3-7, 5-1–5-2, 7-38–7-40, 7-41, 7-43
  routing, 5-1–5-4
IPX, 1-6, 6-1, 6-2, 7-13, 7-14, 7-28–7-33, A-1
  exclusive network, 7-29
  exclusive SAP_type, 7-29
  filtering, 7-29
  frame type, 7-28
  global network, 7-30
  global SAP_type, 7-31
  network numbers, 6-1, 6-2, 7-28
  routing, 6-1–6-3
  Routing Specification, 6-1
Isolate LAN Traffic, 4-6–4-8

J

Jumpers, 2-4, 7-38, B-5

L

LAN Connection, 2-5–2-8
LAN Module, 1-12, B-1, B-2, B-5
LAN Port, 5-1, 6-1
LAN State, 3-6
LAT, 3-8, 4-13, 7-11, 7-13, 7-37–7-40, 7-43, 7-46, A-1, Glossary-4
LAVC, 7-13, 7-14
Learning Phase, 3-2
LED. *See* Indicators
List, 7-15, 7-44, 7-53
Lithium Battery, iii, A-2
Lo, 7-50

L (cont'd)
Local> Prompt, 7-42
  configuring, 7-42
  exiting, 7-50
Lock, 7-40, 7-50, 7-55
Login, password, 7-40
Logout, 7-50

M

Maintenance Password, 7-40
Man, 7-50
Management, 4-13, A-1, A-2, C-1
MAU (Medium Attachment Unit), Glossary-4
Memory Usage, 7-48
Metric, 7-24
MIB (Management Information Base), C-1, Glossary-4
Modular Jack, 2-1, 2-2, 2-6, 7-38, A-1, B-1, B-5
Monitor, 7-15, 7-44
MOPDL, 7-13, 7-14
MOPRC, 7-13, 7-14
Multi-site Operation, 4-3
Multicast, 7-8, 7-37, 7-45, Glossary-5
  timer, 7-41
Multiport Transceiver. *See* Fan-out Transceiver

N

Name (server), 7-41
Nameserver, 7-41, Glossary-5
NETMan, 4-13
NetRunner, 1-9
NetWare, 6-1, 7-13, 7-14, Glossary-5
Network address, Glossary-6
Network Control Program (NCP), 7-40, Glossary-5
Network Number
  IP, 5-1–5-3, 7-25
  IPX, 6-1–6-3, 7-28
NFS (Network File System), 5-2
Node, Glossary-6
  adding to network, 4-4
  definition, 1-12
  number (server), 7-41
Novell, 6-1, 7-13, 7-14, A-1
Number (server), 7-41

O

Operation (normal), 3-3

P

Passwords, 7-39, 7-40, 7-42, 7-50
Ping, 7-51
Point-to-Point Operation, 4-2
Port
  defined, Glossary-7
  lock, 7-40, 7-50
  priority, 4-11
  selection, 2-4, 7-38
  set, 7-52
  show, 7-53
  test, 7-55
  unlock, 7-55
Power-up, 3-1
Priority, 4-11
Privileged, 7-2, 7-42, 7-52
Processes, 7-49
Prompt, 7-42
Protocol, Glossary-7
Purge sysdump, 7-51

R

Receive Failure, 7-47
Reset, 7-50
RFC 1009, 5-1, A-1
RFC 1066, C-1
RFC 1157, C-1
RFC 1213, C-1
RFC 1286, C-1
RFC 1362, 6-1, A-1
RIP, 4-12, 7-23, 7-27, 7-33, 7-36, A-1
  spoofing, 1-7, 1-8, 7-9
RJ45. *See* Modular Jack
RLB (Remote LAN Bridge), 1-9, 4-4, 7-7, 7-8, 7-18
rlogin, Glossary-7
Root Path Cost, 4-11, 7-18, 7-19
Router, 1-9
  interoperation, 4-12
  IP, 5-1, 7-23
  IPX, 6-1
  protocols, A-1
  traditional, 4-12

R (cont'd)
Routes
dynamic, 7-27
static, 7-24, 7-27

S

Safety, ii, iii
SAP, 7-9, 7-33, 7-36
spoofing, 7-9, 7-20
Save, 7-51
Save Configuration, 7-51
Send Failure, 7-47
Server
name, 7-41
status, 7-48
Service, Information, v
Session Port, 7-52, 7-53
Set, 7-5, 7-37
Set Ports, 7-52
Setup (into EasyRouter mode), 3-4
Show, 7-15, 7-44
Show Users, 7-55
SNMP, 3-8, 4-13, 7-13, 7-14, A-1, A-2, C-1–C-37, Glossary-8
Software Compression, 7-8
Software Port Selection. *See* Port, selection
Spanning Tree, 4-10, 4-11, 7-10, 7-16, 7-19
active/passive, 4-11
enabling/disabling, 4-10, 7-10
root bridge, 4-11, 7-18, 7-19
Specific Filter, 7-11, 7-12, 7-14
Startup. *See* Boot-Up
Static Routes, 7-24, 7-27
Statistics, 7-16, 7-17, 7-26, 7-34, 7-45, 7-54
Subnet Mask, 7-43, Glossary-8
Switches, B-2, B-3
Symbols, 1-12
Syntax, 7-1
sysdump, 7-54
System Dump, 7-51, 7-54

T

Tap, Ethernet, Glossary-8
TCP/IP, 1-4, 7-7, 7-38–7-40, 7-41, 7-46, 7-49, 7-51, Glossary-8
Telnet, 3-8, 4-13, 7-11, 7-39, 7-40, Glossary-9
Test, 7-55
Test Port, 7-55
TFTP, Glossary-9
ThickNet, Glossary-9
ThinWire connection, Glossary-9
Traditional Bridge Mode, 3-7
Transceiver, Glossary-9
TÜV, B-2
Twisted Pair Hub, 2-2, 2-5, 2-6

U

UL, B-2
Unit (definition), 1-12, Glossary-10
Unlock Port, 7-55
User Processes, 7-49
Users, 7-54, 7-55

V

VT100, 7-52

W

WAN, 1-12, 2-5, 7-55
address, 7-25
optimize, 7-33
port, 1-12, 5-1, 6-1
WAN Link, 1-12, 3-2, 4-6
Warnings, ii, iii
Warranty, v
Weed Time, 7-10, 7-19
Who, 7-55

X

XNS, 7-13, 7-14

Z

Zero Counters, 7-55

READER'S COMMENTS

MICOM welcomes your evaluation of this manual and any suggestions you may have. These help us to improve the quality and usefulness of our publications.

Manual Name Integration Router User's Manual Part No. 800-1768-60 Rev. A

	Excellent	Good	Fair	Poor
How would you rate the manual overall?	❑	❑	❑	❑
Are the *installation instructions* effective?	❑	❑	❑	❑
Are the *operating instructions* clear and complete?	❑	❑	❑	❑
Is the manual properly *organized*?	❑	❑	❑	❑
Is the *artwork* clear and easy to understand?	❑	❑	❑	❑
Is the *index* useful?	❑	❑	❑	❑

Did you find any errors in the manual? (Please reference page, paragraph, table or figure number)

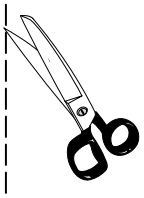
How might we improve this manual?

Name Title

Company Name

Address Telephone ( )

Thank you for taking the time to fill out this form.



PCR 1077D

FOLD AS MARKED AND TAPE CLOSED BEFORE MAILING.
PLEASE DO NOT STAPLE.

Fold Here

From: _____

_____

_____

NO POSTAGE NECESSARY IF MAILED IN THE UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS PERMIT NO. 906 SIMI VALLEY, CA 93062

POSTAGE WILL BE PAID BY ADDRESSEE

MICOM Communications Corp.
ATTENTION: Manager, Technical Publications
4100 Los Angeles Avenue
Simi Valley, CA 93063–9949